NEW ORGANIZED CRIME: PROBLEMS AND ISSUES FOR INFORMATION ANALYSIS

Suleyman Demirci, B.S.

Thesis Prepared for the Degree of

MASTER OF SCIENCE

UNIVERSITY OF NORTH TEXAS

August 2001

APPROVED:

Tory J. Caeti, Major Professor
Robert W. Taylor, Professor and
Chair of the Department of Criminal Justice
Eric J. Fritsch, Committee member
David W. Hartman, Dean of the School of
Community Service
Neal Tate, Dean of the Toulouse School of
Graduate Studies

Demirci Suleyman, New Organized Crime: Problems and Issues for Information Analysis. Master of Science (Criminal Justice), August 2001, 108 pp., 1 table, 1 figure, references, 82 titles.

This study illustrates the changing nature of organized crime at both national and international levels. Organized crime groups have changed in that they have entered the realm of high technology. In response this change, the use of new or modified analytical tools is suggested to enhance law enforcement efforts. This study highlights the problems of, and offers particular solutions for information analysis in its use in the fight against organized crime. Ultimately, it is argued that combined crime and intelligence analysis can be an effective and efficient method for the detection and prevention of modern organized crime.

ACKNOWLEDGEMENT

I would like to thank Dr. Tory Caeti, Dr. Robert Taylor, Dr. Eric Fritsch, Victoria DeWaters, and all of my friends. Through their support and encouragement, my ideas were developed, combined, and refined to form this thesis.

I am grateful for Turkish National Police that financially supported my education and gave me the chance that I have never dreamed of having.

Most of all, I deeply appreciate all Muzehher, Nihan, and my family have done for me in this study.

TABLE OF CONTENTS Page

LIST OF TABLES

Table Page

LIST OF ILLUSTRATIONS

CHAPTER I

INTRODUCTION

Technological developments have changed the nature of crimes throughout the world. Criminals interact more with one another with the assistance of advances in information technology (Freeh, 1999). Organized crime groups have also begun to perpetrate different activities all over the world. These groups have become increasingly networked through the Internet and other communication tools (Williams, 1995). This is a natural result of globalization. This change has required modifications in police tactics. As Swanson, Territo, and Taylor (2000) note, law enforcement efforts have changed from reactive policing to proactive policing in last two decades. While reactive policing refers to street level policing and instant responses to criminal groups in a short term, proactive policing attempts to define long term goals, including general patterns and future trends of criminal activities. Particularly, proactive policing has a key role for the success of organized crime prevention. Further, crime and intelligence analysis are considered essential tools to establish preventive strategies for organized crime (Fahlman, 2000).

This study considers about the movement of organized crime activities from traditional to cyber-oriented crime. Due to this shift, law enforcement units have faced the flow of vast amounts of information, including bank records, court records, and other business records (Albanese, 2000). Therefore, the study addresses the critical role of crime and intelligence analysis. Although the purpose of crime analysis is to examine the general patterns of crime, Geographical Information Systems (GIS) as a means of crime

analysis integrates both crime and intelligence analysis techniques, including pattern analysis and link analysis. The combination of these analyses is considered to be a powerful and efficient tool for decision-making about organized crime preventive strategies. This study examines the literature on information analysis while focusing on the change in organized crime at local, national, and international levels.

Overall, this paper posits that the changes in organized crime activities require the modification of current law enforcement efforts. Therefore, this study addresses the analytical methods to handle the difficulties of organized crime prevention. These techniques are considered supportive tools to help the decision making process effective and efficient, and to establish effective organized crime policies.

Statement of the Problem

Modern organized crime activities have begun to exploit the benefits of information technology. Their use of these technologies renders digital information. For instance, infinite number of money transactions among criminal organizations indicates such information. The problem is that now, information from various sources flows into law enforcement records. For this reason, law enforcement agencies must utilize new and powerful analytical techniques to decipher this information. Accordingly, police managers must take these issues into consideration while considering cost-benefit analysis and information privacy aspects. Briefly, the problem requires the handling of information via current information systems.

Purposes of the Study

The purpose of this study is to offer the combination of crime and intelligence analysis as a means of information analysis for establishing organized crime prevention strategies. This study does not address organized crime policies and other law enforcement efforts. Further, this study attempts to integrate GIS and crime mapping, and other intelligence analysis techniques, such as network analysis, telephone record analysis, and financial (worth) analysis through specific examples. Finally, this paper identifies and offers solution to problems with information analysis.

Research Questions

This study attempts to answer the following research questions:

1. How do organized crime groups engage in cyber-oriented crime?
2. Why have law enforcement agencies been very slow to share information regarding organized crime activities?
3. What is the proper mechanism to analyze organized crime information?
4. In what ways are information analysis techniques likely to be adopted into law enforcement's organized crime intelligence environment?

Limitations of the Study

The main topics handled in this study are organized crime, intelligence analysis, problems, and solutions for information analysis. Confidentiality is another limitation. Illustrative examples for each proposed analysis method may not be available, because

real-life examples include top-secret or confidential information. In addition, the meaning of organized crime changes from one country to another, from one agency to another, and so on. Therefore, the limitations of this study can be classified as follows; lack of an all-encompassing definition of organized crime, and the lack of empirical study on organized crime.

Organized crime has many distinct definitions depending on the purpose, agency, and geography. In other words, while some define organized crime as any conspiracy among two or more people, others focus on particular characteristics to indicate organized criminality, such as extortion, violence, and corruption. Scholars and agencies such as the FBI and Interpol all have considerably different definitions of organized crime. Because it was not possible to measure the validity and reliability of definitions changing regarding to the purpose, agency, country, and geography, there is no unique or single definition of organized crime. The lack of definition not only challenges the comprehension of organized crime, but it also makes the working investigative definition ambiguous in law enforcement applications.

Another issue regarding organized crime is that most books and sources represent the mystical aspects of organized crime. This information may be completely invalid; therefore, someone who deals with organized crime must be selective in choosing source information. The mystical information must be separated from valid sources. In addition, there is a limitation in getting information on organized crime in that the only empirical information about organized crime comes from law enforcement units. This information

may be difficult to acquire. This makes the resources limited to journal articles which may not be fed by experimental works.

Writing about criminal intelligence requires a higher level of confidentiality than many other studies in criminal justice. In fact, because intelligence units are disciplined with top-secrecy, it is difficult to measure the applicability of analytical methods mentioned in the study. In other words, consistency of the methods for organized crime may not truly be measured without having illustrative cases in which intelligence analysis techniques were used. The only method achieved here is the analysis of the cause and effect relationship in the information obtained from different sources. Comparing and contrasting the points stressed in different articles was found to be a useful way of analyzing the information used for this paper.

Overall, crime and intelligence analysis may be achieved by information that is gathered from numerous amounts of resources. If Government does not permit law enforcement to use this information, these analyses are more likely to be ineffective. Indeed, this is one of the biggest limitations for this study and information analysis.

Methodology

This study is a comprehensive literature review. Synthesizing the related information makes this paper unique. This study was conducted using a number of steps. First, this study firstly examined the dynamic nature of organized crime. There were many critical points that are expected to make research on it. However, this study does not deal with entire organized issues. On the other hand, most of scholars were

addressing the importance of intelligence analysis on organized crime. This has been considered powerful tool in organized crime prevention.

However, this study decided that intelligence analysis, dealing with the relationships among the criminal members, may not be enough to establish effective strategic policies against organized crime. Therefore, this study attempted to combine crime and intelligence analysis techniques for the effective prevention programs. Indeed, these two analyses are expected to support the policy makers.

This study realized that international law enforcement organizations, such as UN and Europol, have applied global mapping projects to establish the general patterns and future trends of organized crime regarding the relationship between geographical location and crime. This basically refers to environmental criminology. In this consideration, this study added some practical applications for information analysis in local, national, and international organized crime prevention efforts. These are: RISS, Mapping organized crime activities, etc.

Overall, the information provided in this paper was located through extensive library and Internet searches. In synthesizing this information, I hope to show the need for the use of combined crime and intelligence analysis (CIA) in the effective detection and prevention of organized crime.

This paper is comprised of six chapters: Introduction, Changing Nature Of Criminal Activities And Law Enforcement Efforts, Information Analysis in Law Enforcement, Problems in Information Analysis, Solutions for Information Analysis Issues, and Conclusion.

The second chapter focuses on the changes in organized crime activities in the world. Then, it addresses the imperative modification in law enforcement efforts against organized crime. According to the literature, law enforcement has been successful in gathering information on organized crime (Rucker, 1995). Law enforcement has also been successful in fighting organized crime around world (Dintino and Martens, 1981). However, organized crime is still a major threat to society and international security. The activities of organized crime are changing and are moving toward high-tech crime such as computer fraud and money laundering (Freeh, 1999). These new tendencies of organized crime are becoming more transnational due to the technological innovations in communication, transportation, and electronic money transfer. Thinking about these developments, the job of law enforcement is becoming more difficult. For these reasons, law enforcement forces should be more proactive through the process of organized crime prevention. This chapter also stresses the importance of international law enforcement agencies, such as United Nations, Europol, and Interpol. In short, chapter two addresses the importance of information management in this endeavor.

The third chapter contains a comprehensive literature review of information analysis. Because the previous chapter addresses the significant role of information, this chapter focuses on information analysis for the effective management in law enforcement. As mentioned earlier, the activities of organized crime are not stable. While some groups deal with drug trafficking, counterfeiting, and gambling in traditional forms, others may try to penetrate legitimate business to act as businessmen, to become involved in electronic commerce, and money laundering in order to make their income “legal”.

Due to the diversity of activities, law enforcement has faced a huge amount of information regarding organized crime movements. However, having massive amounts of information is not enough to solve the problem of organized crime. According to Dintino and Martens (1981, p.56), logical analysis is required, and they add, “There is no simple answer or solution to the problem of organized crime”.

The fourth chapter concentrates on particular issues relating to organized crime, and information analysis, including technological issues, privacy and security issues, and managerial issues. Technological issues refer to costs, expertise, and data quality, and privacy and security issues are examined together. Finally, this chapter stresses the problems that the police management has faced due to the particular needs of information analysis and its users.

The fifth chapter offers solutions for problems mentioned in the previous chapter. These solutions are addressed under the headings: Managing information and technology, Privacy Issues, Educational Issues, Sharing among International Organizations, and Managerial Issues.

CHAPTER II

CHANGING NATURE OF CRIMINAL ACTIVITIES AND LAW ENFORCEMENT EFFORTS

Introduction

The amount of information available to investigators detecting and policing organized crime has increased dramatically due to changes in organized crime activities. These activities have changed through recent technological advances in local, national, and international communication networks. Included in these advances are the Internet and other communication devices. Such advancements have allowed organized crime groups to enter the digital world, and exploit new opportunities to increase profit in this digital environment. Further, their activities have become transnational due to globalization of information (Shelley, 1995).

The evolving nature of organized crime means that law enforcement units now must face a growing amount of information; including financial records, public records, and a variety of open sources related to or on the Internet. Such information complicates police responsibilities. Dintino and Martens (1983) state that a critical and thoughtful analysis is required for comprehending the nature of organized crime. In other words, due to its complex nature, the problem of organized crime cannot be solved by implementing straightforward solutions.

Law enforcement has been faced to change its tactics and methods to address these new types of criminal activities. In short, this chapter reviews the change in the

activities of criminal organizations, and the changes in police efforts against organized crime.

New Trends In Organized Crime Activities

In this section, organized crime is addressed with a focus on the transition from traditional crime to cyber-oriented crime.

Understanding Organized Crime

Organized crime has maintained its controversial nature since the first identifiable organization, the Sicilian mafia. Before identifying new trends in organized crime activities in 21st century, definitions and theoretical perspectives of organized crime are examined. However, there has been no single, agreed upon definition of organized crime.

From the criminologists' point of view, the key factor to identify the reasons of organized criminality is the sociological problems and unequal opportunities in society. According to criminological theories, organized criminality occurs due to poverty and cultural or ethnic reasons (Milhaupt & West, 2000). Bovenberk and Yesilgoz (2000) state that criminological theories have failed to analyze the real nature of organized crime. Criminological theories do not explain why organized crime emerged. Not all persons from an impoverished background are involved in organized crime. Also, many persons involved with organized crime came from wealthy backgrounds (Abadinsky, 1997). According to Bovenberk and Yesilgoz (1998), there are two major reasons why theories have not been successful in describing organized crime. First, most criminological theories have focused on individuals. They ignored groups and the network of connections between groups. Second, criminological theories deal with specific crimes

that official institutions have defined as illegal. The crimes addressed in these theories do not include crimes, such as computer crime or organized criminal activity.

On the other hand, law enforcement agencies identify organized crime from their perspective. For instance, the FBI defines organized crime as;

> " Any group having some manner of formalized structure and whose primary objective is to obtain money through illegal activities. Such groups maintain their position through the use of violence or threats of violence, corrupt public officials, graft, or extortions, and generally have significant impact on the people in their locales or regions of the country" (Abadinsky, 1997, p.3).

Organized crime has specific characteristics which are different than ordinary type of crimes, such as robbery, assault, and shoplifting. Abadinsky (1997) defines organized crime as "a nonideological enterprise that involves a number of persons in close social interaction, organized, on hierarchical basis for the purpose of securing profit and power by engaging in illegal and legal activities" (p. 13). Albanese (1996) defines organized crime as "criminals organized into illegal firms…operating in such criminal fields as loansharking, prostitution, gambling, and narcotics but also in legitimate fields as well, and employing violence and the corruption of police as key business methods" (p.3). Additionally, Levi (1998) describes organized criminality by its common characteristics, including violence, corruption, continuity, and involvement in a number of different criminal activities.

Due to the disparities between the different definitions of organized crime and for the purposes of this study, the definition "a continuing criminal enterprise" will be used. This definition addresses the dynamic structure of organized crime, and it treats

organized crime as a business. This description implies why organized crime groups enter legitimate business today to profit.

Manning (1999) discusses the pattern of organized crime activities in four phases of development. The phases he posits are: tactical crimes, illegal business activities, legitimate business, and big business. Activities within each stage are presented in the table below.

Tactical crimes	Illegal Business	Legitimate Business	Big Business
Arson	Counterfeiting	Auto agencies	Banking
Assault	Frauds	Factoring	Construction
Bribery	Gambling	Food products	Credit cards
Burglary	Illegal alcohol	Garment manufacturing	Entertainment
Corruption	Loan sharking	Night clubs and bars	Hotel and motels
Extortion	Narcotics	Trade unions	Insurance
Hijacking	Prostitution	Trucking	Labor
Murder	Protection rackets	Vending machines	Real estate
Robbery	Smuggling	Waste collections	Securities
	Stolen property		

Table 1.1. Organized crime activities, modified from: Manning, G.A. (1999). Financial investigation and forensic accounting. London, UK: CRC Press.

Organized crime groups entered the business world to launder money from illegal ventures, all the while continuing their involvement in tactical crimes. The following section addresses the recent change in organized crime activities. The reasons for the changes are also addressed.

The Organized Crime Shift: Traditional to Cyber Crime

Organized crime is increasingly becoming a threat to societies around the world (Godson and Olson, 1995). These groups have become more interrelated and have

crossed national borders by means of technological advances in communications. Criminal organizations have entered the high-tech realm to maximize economic profit. These recent trends have made the nature of organized crime much different than it has been in the past. In fact, organized criminal activities today are considered to be international threats as well as national problems (Brandt, 1995).

Albanese (2000) notes that criminal organizations always attempt to exploit new criminal opportunities. For instance, technological tools, such as internet and other telecommunication systems empower organized criminal actors to achieve their goals--money and power. Because these criminals are using high-tech devices and techniques, organized crime has become a global problem. Criminal organizations may network with one another via Internet. As one of the most powerful products of technology, the Internet may facilitate organized crime in penetrating legitimate business, and in manipulating financial institutions (UN, 1999).

The creation of global consumer markets encourages the growth of organized crime in quite a lot of ways. First, as in multinational corporations, these new transnational markets are open to all, including criminal organizations. Second, criminal organizations may be better suited to exploit these opportunities than traditional and legitimate corporations. Criminal organizations have expertise in operating outside the law, outside regulations and outside norms of business practice. These groups have few qualms with abandoning legal niceties when violating international borders. Criminal organizations operate outside the existing structures of authority, and they have already

developed strategies for circumventing law enforcement both in individual nations and across international boundaries (Williams, 1995).

Carter (1998) addresses the convergence of four main crime trends:

- Organized crime
- Industrial espionage
- Violent crime
- Computer crime

The convergence of these types of crimes also supports the idea that the activities of organized crime groups have changed dramatically. According to the project report "Strategic Study of RCMP Economic Crime Program", "The most important enterprise crimes in the future will be international financial fraud, commercial fraud, money laundering, and tax evasion." (Carter, 1998, p.5).

Change in Law Enforcement Efforts

In the development of criminal investigation methods, there have been two distinct approaches for fighting crime in the US; reactive and proactive (Swanson, Territo, and Taylor, 2000). In the past, reactive techniques were the most commonly used in fighting criminal organizations, while contemporary techniques focus on proactive approaches. In other words, predicting crime and the future activities of criminal organizations is more important now than before in law enforcement applications. Due to the movement into cyberspace, massive amounts of information exist regarding organized crime activities both locally and internationally. This information may be obtained from credit card records, financial transactions, and other additional sources on

the Internet. However, this information may not be sufficient evidence in cases against organized criminals. Investigators must combine information from cyberspace with information obtained through traditional techniques. Integrating this information can clarify the complex nature of organized crime.

Peterson (1994) argues that crime and intelligence analysis are essential tools in investigating complex organized crime, analyzing information, creating strategic assessments, and supporting managers and policymakers. In explaining proactive policing, Maguire (2000) points out this approach is a result of a combination of intelligence-led policing, information sharing between agencies, and risk management. Sharing information and risk management are based on problem-oriented policing and partnership. Recently, the term "criminal business analysis" has been used to address these aspects of policing (Maguire, 2000).

In 1993, the United Kingdom Audit Commission identified some organizational barriers to effective policing. They found little integration in crime fighting efforts. The report also argued that police resources were not being used efficiently. Finally, they found that the emphasis of investigation was on crime instead of on criminals. The Audit Commission recommended that police be more proactive by using a number of approaches, such as numerous informants and other intelligence gathering and analysis techniques (Gill, 1998).

Traditionally, arrest rates were used to measure the success of organized crime policing. However, Gill (1998) argues that arrest and prosecution percentage rates cannot be a valid measurement of intelligence-led policing. Nonetheless, managers can use such

rates to identify organized criminal activities that have not been previously identified. In other words, managers can evaluate evidence of possible organized crime activities so they can quickly respond to these activities (Schneider, 1994). In this manner, the recent crime reduction model should be replaced with traditional "arrest-confession" strategies (Gill 1998).

The methods used in intelligence-led policing require taking some risks. Maguire (2000) states that intelligence-based investigation techniques, including the use of electronic surveillance and informants, can only be accomplished through a sophisticated process of risk management and risk assessment. In such cases, raw material is information, and police agents are one of the most important resources. In other words, police agents act as communicators in the exchange of risky knowledge. Therefore, law enforcement agencies must recruit proper personnel to perform such tasks as collecting, analyzing and disseminating information. The main focus of this study is the effective analysis of information through crime and intelligence analysis techniques. These techniques are discussed next.

The Shift from Reactive to Proactive Policing

The use of intelligence-led policing (proactive policing) has been growing in law enforcement for several reasons (Gill, 1998). The first reason is transnational developments, such as international criminal networks and relationships. The changing nature of organized crime is another factor that has caused the shift to intelligence-led policing. Transnational organized crime has had a particular impact on this trend. Finally, intelligence-led policing provides new police strategies and analytical methods. In order

to develop police networks at the national or international level, the proactive role of intelligence plays an important role.

The major concern in proactive policing is to predict future activities of criminal organizations. Proactive policing and long term policing, will be referred as intelligence-led policing in this section. Such policing provides information that may require specialized analytical methods to express the evidence in courts. In other words, prosecuting organized criminals entails analytical and visual methods to persuade judges, juries, and prosecutors (Sheptycki, 2000). If law enforcement agents can utilize the specialized analytical methods required to investigate organized crime, they should also be able to clarify the organized crime problem in the courts. In contributions to intelligence-led policing, policy makers can create new and effective programs and direct law enforcement toward new strategies in the fight against organized crime. (Gill, 1998).

Although traditional law enforcement has been successful in collecting information through street-level investigations and undercover operations, this information has limited value for controlling sophisticated crimes like organized crime (Dintino and Martens, 1981). Intelligence-led policing requires the efficient use of informants, and the use of specialized tools to analyze organized crime cases. In spite of technological advances, such as police surveillance technology, informants have remained a crucial element in fighting organized crime (Sheptycki, 2000). In intelligence-policing, raw information is converted to efficient and useful knowledge.

Rising crime rates and decreasing crime detection rates require some changes in more traditional police applications (Maguire, 2000). The systematic and frequent use of

informants and surveillance techniques are increasingly being used in police investigation operations. The reason for this change is that involving informants in an operation is less expensive than technological intelligence even if it is more dangerous (Norris and Dunnighan, 2000). One of the major risks of using informants is informant corruption. Another risk is that they may be working for both the police and the criminal organization. Sheptycki (2000) states that one of the functions of intelligence-led policing is to balance the use of human intelligence and technical intelligence. In other words, they have equal significance in intelligence operations. Managers should be aware of the appropriate uses of each type of intelligence.

Maguire (2000) focuses on several characteristics of intelligence-led policing. He ties proactive methods to the use of information gathering, analytical and investigative tools and techniques, as well as undercover operations, criminal informants, bugging, and visual surveillance equipment. Financial tracking and computer facilities are also involved in this type of policing. He argues that intelligence-led policing requires free exchange of information, which has historically been considered secret between police and other public agencies. Proactive policing also provides law enforcement with both formal and informal techniques that have not been used in criminal justice and penal systems. Finally, at the organizational level, all activities and operations are considered "business plans", "targets", and "performance indicators". In other words, teamwork and specialized skills and functions are developed (Heaton, 2000). Combining skills and information is seen as much more efficient than traditional police methods.

Although proactive policing offers many techniques for investigating organized crime cases, this study focuses on the specialized methods used to analyze raw information. This raw information can become viable knowledge using the methods explained in the next chapter.

Need for Information Management and Analysis

Up to now, the movement from traditional to cyber-oriented organized crime has been emphasized. It was added that police have been able to obtain massive amounts of information due to this movement. This does not mean that investigating these crimes have become easier than before. Conversely, it may be more difficult to establish the relationships between organized criminals with this information unless specific analysis methods are used. As mentioned earlier, because organized crime has become a global problem, local solutions will be ineffective in preventing organized crime. Levi (1998) states that organized crime prevention must be considered on an international level but carried out locally. For this to work, there must be a mechanism in place to facilitate cooperation and information sharing between agencies and countries. If this mechanism can be developed between local and international law enforcement agencies, massive amounts of information from numerous resources may flow. In this picture, information management plays an important role to exchange of proper and reliable knowledge between agencies so that organized crime prevention efforts operate properly.

One of the essential tools in the prevention process is effective criminal intelligence. Criminal intelligence organizations must have a process of systematic data collection, evaluation, analysis, and dissemination to address data from a wide variety of

sources and to identify future trends and patterns (Stewart, 2000). These organizations must also be capable of preparing threat assessment before events occur.

The processing of intelligence plays crucial role in making predictions and enhancing future-oriented and problem-oriented policing. Godfrey and Harris (1971, p.9) argue that criminal intelligence can "detect and anticipate criminal trends that will put law enforcement in the position of initiating long term action, rather than merely reacting to criminal behavior." In recent years, law enforcement agencies and intelligence units have been converging to address organized criminal behavior intelligence. Alliances are important for solving complex crimes such as international organized crime, illegal immigration, and money laundering. These types of crimes are becoming the focus of intelligence gathering in law enforcement agencies (The Intelligence Community in the 21st Century, 1996). The Intelligence Community in the 21st Century report emphasizes that information management should be established between these two communities. Although there are several differences between these agencies in terms of rules, regulations, objectives, and their methodologies in collecting data, a common understanding and language, such as crime and intelligence analysis, is likely to facilitate intelligence sharing among them. To achieve this, the minimum requirement is that an intelligence unit be established and dedicated to the flow of raw information (Maguire, 2000).

In short, law enforcement units at local and international levels must address the management of information. New information technologies are considered crucial in this process. For instance, sophisticated database programs, GIS (Geographical Information

Systems) software programs (MapInfo, Arc Info, Arc View, etc), and link analysis programs (I2) are essential components of this information management.

View of International Law Enforcement Organizations

As explained earlier, organized crime is no longer a simply localized problem. In the age of global information, organized crime is an international concern. Countries cannot be unaware of or ignore this controversial issue. Therefore, The United Nations, Europol, and Interpol have stepped in and have begun to use information analysis methods for sharing knowledge among the countries.

According to reports presented by The Institute for Security Studies Western European Union (ISSWEU), organized crime and drug trafficking are visible enough to trace their activities regarding to areas in which authority of state is challenged (Politi 1997). The ISSWEU offered a "geo-strategy" to struggle against both organized crime and drug trafficking. Geo-strategy provides law enforcement with an international picture of organized crime activities. Differences in laws and procedures between countries are identified, and ways to integrate and unify policies and investigative methods are examined. The big picture indicates the contest of states' authority in such areas that are clarified by maps (United Nation, 1999). Mapping organized crime activities has two significant uses. First, it allows agencies to visualize the global and regional level of organized crime and drug trafficking. Second, and more importantly, it links the problems and issues of these types of crime. As one of the most important analytical methods, mapping will be discussed in the next chapter.

The United Nations has also begun mapping criminal activity. Their project is to map global activities of international organized crime groups while considering the level of impact on global security. This mapping enables the monitoring of trends and patterns, it allows for forecasting future activities. Therefore, prevention techniques against global organized crime may be developed and implemented (UN, 1999). Additionally, mapping these diverse activities may allow law enforcement agents to measure the reliability and accuracy of new information.

Europol and Interpol are assisting in the development of methods agencies may use to communicate with one another (Europol, 1998). Therefore, Europol and Interpol are offering crime and intelligence analysis methods for the countries concerning organized crime problem. They believe that exchange of information and intelligence can be facilitated only through these methods. Every law enforcement agency must communicate using the same methods. These agencies must use the same documentation and format to facilitate this information exchange. Therefore, Europol and Interpol consider the CIA (Crime and Intelligence Analysis) program to be a key element in the sharing of information (Fahlman, 2000). It is clear that international law enforcement organizations understand the significance of CIA. These organizations have been able to accomplish information sharing among different agencies and this has led to successes in policing of organized crime.

Conclusion

This chapter has presented the significant changes in organized crime activities and law enforcement efforts to combat them. Law enforcement efforts must be improved,

and their tools and techniques must at least match those need by criminal organizations. Effective strategies for addressing organized crime must take into account the dynamic nature of the various types of activities engaged in by these criminal groups. Comprehensive data, based on law enforcement and court information, can support policy makers in harmonizing laws and policies addressing organized crime. Nevertheless, if police agencies cannot analyze information in an effective way, it will not provide any useful clues for policy makers engaging in organized crime prevention. The next chapter focuses on information analysis, including crime and intelligence analysis.

CHAPTER III

INFORMATION ANALYSIS IN LAW ENFORCEMENT

Introduction

Law enforcement agencies utilize criminal intelligence in their daily activities. The information explosion, changing technology, and increasingly global organized crime activities mean that there is an increasing need to develop more systematic methods of crime analysis and intelligence analysis. Besides improving crime and intelligence analysis techniques separately, law enforcement agencies must integrate these techniques together for both tactical operations and to develop policies for organized crime prevention.

The changing nature of organized crime has spawned new challenges for law enforcement agencies in recent years. The global marketplace exists without boundaries or borders, and it fosters the free flow of money. Electronic financial transactions, the Internet, and cellular and satellite communications assists people in living an efficient life. Criminal groups also utilize these technologies in their activities. The use of high technology has made organized crime activities much more complex than in the past. Criminal organizations can easily exploit electronic transactions to hide their activities and launder funds (Fahlman, 2000). With organized crime groups exploiting this global and digital arena, law enforcement must develop and redefine the means of controlling and preventing organized crime.

There are five important areas to consider when looking at organized crime: managing the intelligence and investigation processes, obtaining evidence, coordinating investigations, proactive policing, and the policy-making process (Europol, 1998). When one considers information analysis in law enforcement applications, crime and intelligence analysis must be handled together. Crime analysis, specifically, deals with crime patterns and trends for a specific area, while intelligence analysis focus on the relationships between criminals and within their organizations. As mentioned before, organized crime groups commit various types of crimes, depending on their locations (Albenese, 2000). Organized criminals have also become much more networked with one another (Levi, 1998). Therefore, both analyses are considered essential tools for organized crime investigation and prevention. Using crime analysis and intelligence analysis together increases the efficiency and reliability of information. This chapter concentrates on crime and intelligence analysis techniques. Specifically, GIS and crime mapping are considered as the focal points of crime analysis. Link, worth, and telephone record analysis will be considered as the cornerstones of intelligence analysis techniques for organized crime prevention.

Crime and Intelligence Analysis

This section covers both crime and intelligence analysis applications for organized crime prevention. Definitions of crime and intelligence analysis are presented along with formation on technical level, and their current applications to organized crime. These analyses, when combined, establish a proper mechanism for information

management and sharing among local, national, and international law enforcement agencies.

Crime Analysis

Crime analysis may be defined as "a set of systematic, analytical processes directed at providing timely and pertinent information relative to crime patterns and trend correlations to assist operational and administrative personnel in planning the deployment of resources for the prevention and suppression of criminal activities, aiding the investigative process, and increasing apprehensions and clearance of cases," (Gottlieb, Arenberg, Singh, 1994, p.13). Thus, the goals of crime analysis are: processing information in a timely manner, and preventing and controlling crime based on accurately processed information. According to Reuland (1997), crime analysis identifies " trends and patterns within crime data in an attempt to solve crimes or prevent their repeat occurrence " (p.53). In a contemporary crime analysis unit, there are three distinct areas of analysis: strategic crime analysis, tactical crime analysis, and administrative crime analysis (Haley, Todd, and Stallo, 1998). These methods are presented below.

Strategic Crime Analysis

In strategic crime analysis, analysts are concerned with the future trends of crimes and the quantitative measurement of a wide range of crimes (Godfrey and Harris, 1971). Crime trend forecasts, resource allocation, and situational analysis are also involved in this category (Haley, Todd, and Stallo, 1998). Future crime tendency projections are based upon past and current information so that managers can make smarter decisions in the planning phase (Schneider, 1994). Resource allocation analysis uses a cost-benefit

analysis to verify the best possible use of personnel for maximum efficiency (Stallo, 1997). Situational analysis offers beat profiling planning by using demographic data including victims' experiences (Rossmo, 2000).

Tactical Crime Analysis

Tactical crime analysis can be classified into three categories. Crime pattern/series deals with separate events and analyzes crime patterns in terms of day/time, location, clusters, and previous similar crimes. Using these analyses makes it easier to predict areas of need and to direct human resources. Crime-suspect correlation is a process that provides correlational data between possible suspects and particular crimes. The correlation may be obtained by analyzing criminal histories and other intelligence data supplied by other agencies and sources. Finally, crime analysis develops target-suspect criminal profiles in order to better examine and scrutinize specific types of offenders, such as sex offenders. This kind of data may also be used to take proactive steps to control crime in a community (Haley, Todd, and Stallo, 1998). From the perspective of intelligence analysis, tactical analysis supports current law enforcement operations to make them more successful (Schneider, 1994).

Administrative Crime Analysis

Administrative crime analysis studies policy development and the rationalization of the use of resources (Gottlieb, Arenberg, Singh, 1994). This type of analysis results in the creation of reports such as annual crime reports. The complexity of organized crime requires the more sophisticated analyses and techniques used in strategic intelligence. In this manner, both crime analysis and intelligence analysis techniques are considered

necessary methods for controlling organized crime. For example, crime mapping can be applied to identify the frequency and locations where drug trafficking occurs. Thus, administrators may plan more efficiently and cost effectively. A more detailed discussion of criminal intelligence analysis will follow, including in depth looks at intelligence-led policing, intelligence function, and some major analytical techniques used against organized crime.

Reuland (1997) identifies the four essential tasks of the modern crime analysis unit as: analyzing crime and criminals to determine the allocation of resources, assisting investigators in identifying crime-suspect relationships, accurately reporting crime trends and patterns, and assisting with the prevention of crime. One of the most significant functions of crime analysis is to proactively prevent crime or to support crime control and prevention. Moreover, crime analysis helps to reduce the response time for the police operations.

Crime analysis units are established considering the aim of law enforcement and types of crimes being investigated. Large agencies often divide their crime analysis units into specialized units focusing on narcotics, forgery/fraud, homicide, and intelligence. Therefore, the function of crime analysis changes depending on the department in which it is conducted. In short, crime analysis benefits from the advantages of both tactical and strategic policing in terms of effectively deploying law enforcement resources. Crime analysis may be developed and made more effective with technological innovations, such as GIS. GIS is discussed next, as it is one of the most important innovations in crime analysis.

GIS and Crime Mapping

Crime mapping is a well-known analytical method in many law enforcement agencies, especially in police departments. Mapping is not a new tool, but technological advances have increased its importance in crime analysis. In one of the most important technological advances, GIS can be utilized in crime analysis applications. GIS has changed a traditional form of crime analysis into more flexible and intelligent form. One of the most significant contributions of GIS is that it may integrate information from many sources into one user interface (Olligschlager 1997).

In contrast to traditional pin maps, computerized maps developed by GIS are much more adaptive. They may provide law enforcement agencies with a powerful analytical tool. Computerized crime mappings are considered a powerful analytic method for the analysis of information (Rossmo, 2000). For instance, mapping may be an indispensable tool for analyzing the dispersion of drug carriers and users according to geography in narcotic operations (Gottlieb, Arenberg, Singh, 1994). It is, therefore, possible to predict potential trends of criminal organizations. Even in immediate operations, GIS can be an effective tool to direct operation teams with regard to place, time, and number of persons. Rossmo (2000) suggests the use of computerized maps for geographical profiling, visualizing the trends and patterns of crimes regarding to place, and to aid in successful investigations. Organized crime operations, and most other crime types may be profiled geographically with computerized mapping. While theoretical innovations in organized crime prevention have been important, computerized crime mapping and other information systems have become invaluable in the struggle against

organized crime (Police Foundation, 2000). GIS is the most important component used to upgrade records and see the emerging trends of crime.

Crime mapping has many uses ranging from analyzing information to the proper deployment of personnel, for crime analysis (Dempsey, 2001). The most common use of mapping is in the graphic representation of crime occurrences. This allows law enforcement agencies to recognize the current or future trends of crime types and the activities of criminal organizations. Areas with dense activities are called "hot spots" in GIS applications (Rossmo, 2000). As an example, mapping drug arrests may indicate a growing number of drug dealers in a specific area. With this pattern information, law enforcement agencies may be more effective in the use of their resources.

Describing GIS

A GIS is an automated database that stores, analyzes, and displays both spatial and non-spatial data (Anselin, at al, 2000). GIS is a huge information management system in this definition. Spatial analysis involves the analysis of data in the context of its geographical features. These relations show patterns and trends of criminal activities with regards to location, and it shows coordinate information. Coordinate information details the exact location of incidence or activity. GIS is also capable of comparing this spatial information with information from various law enforcement agents. Therefore, different types of data may be captured and overlaid in GIS software, including political, technological, and social factors. This allows law enforcement to combine various data and process that data quickly. Specialists and managers engaging in organized crime

prevention use GIS in combining theoretical innovations and information analysis in law enforcement.

Applications of spatial analysis in GIS are categorized as either tactical or strategic analysis (Bennecke 1997). The former allows law enforcement to deploy personnel to specific places for specific purposes for police operations. Strategic spatial analysis allows for reports gathered from different regions to be used for future planning, including personnel recruitment and deployment of other resources. If salaries and other operating expenses have been considered, the significance of handling spatial analysis may be understood clearly. Particularly, in using GIS, strategic spatial analysis may augment the efficiency of personnel management. Various techniques have been improved to analyze clusters of data within GIS. Mapping hot spots is included in these techniques.

Utilizing hot spots in mapping is an important tool in crime analysis. A hot spot is "a condition indicating some form of clustering in spatial distribution" (Harries, 2000, p.112). The analyst must be aware, however, that environmental conditions may affect criminal activity. If this is not considered, mistakes may be made in personnel deployment. Because of this, there is no absolute definition of hot spots. Many specialists and researchers have defined hot spots in different way. For instance, Sherman (1995) described hot spots as particular areas in which crimes occur frequently and are predictable. This definition does not include time frame, so it ignores that hot spots occur in a specific period of time. Hot spot analysis may not be useful without considering time factors. Canter (1995) revises this definition and identifies three important criteria:

frequency, geography, and time. He notes that at least two types of crime must be examined in order to label an area a hot spot. A detailed presentation of hot spot mapping is not within the scope of this study.

More technically, GIS provides geo-base files. Contrary to conventional database systems, GIS records information in layers instead of in tables, but GIS can also utilize a tabular format to relate this layered information. All files involved in GIS are established by geo-base which means it stores data in layers. What is the difference between a layer and table? The most essential difference is that a layer can hold information geographically instead of in rows. Objects within the layers are supplemented with geographical coordinates. Olligschlaeger (1997) explains three kinds of data objects, including points, lines, and polygons. In the GIS environment, different symbols are used for different geographical objects, such as radio towers, water lines, and neighborhood boundaries.

Briefly, GIS allows for spatial imaging, database management, decision modeling, and design and planning. Computer mapping is used for identifying spatial or non-spatial data. GIS graphically represents patterns and trends of crimes in a jurisdictional area. In the next section, GIS is discussed as a tool in fighting organized crime activities.

New Trends in GIS Applications

GIS represent different spatial distributions of data and, more importantly, overlaying data to identify interrelated points (Harries, 2000). Recently, GIS applications for crime analysis have been improved with sophisticated technology and by integrating

different technologies. These developments include GIS/GPS (Global Positioning System) integrated systems, Artificial intelligence systems, and three-dimensional mappings. For instance, GIS has been used with GPS which identifies where you are on the earth in terms of coordinates. GPS shows the place as a point with an accuracy of +/- 25 meters (Harries, 2000). This new technology integrated with GIS supports near real-time data collection and analysis (Sorensen, 1997). In emergency cases, the ability to utilize the integrated system reduces response time.

Artificial intelligence applications are considered another turning point in GIS solutions. Law enforcement agencies must anticipate the emergence of criminal activity. In one application, the Pittsburgh Bureau of Police developed an early warning system using GIS and an artificial neural network to forecast the emergence of drug hot spot areas (Olligschlaeger, 1997).

In crime mapping, crime distributions and longitudinal patterns are presented in two dimensions. Two-dimension mapping may not be enough to describe the complexity of crimes in this information storm. Recent developments in computer technology exploit new techniques to address this shortcoming (Lodha and Verma, 1999). Virtual Reality Modeling Language (VRML) may animate complex crime maps and make them more useful. This technique supports three-dimensional maps. Because most of GIS programs do not allow for three-dimensional animation, Integrating VRML and GIS may be an extremely useful tool in the analysis of complex crime maps.

Intelligence Analysis

Information is considered the lifeblood of success in intelligence analysis. As previously noted, various types of information flow into the law enforcement and intelligence agents. New sources of information are arising constantly. In the IC21 form (1996), it is emphasized that as intelligence becomes an indispensable tool for policy makers of organized crime prevention, intelligence capability and essential processes must be adopted for new types of criminal activities. Indeed, this form addresses emerging information sources, and predicts the explosion of available information. Besides crime analysis, intelligence analysis techniques must be considered, and technical personnel must design and implement new models for intelligence analysis.

General Overview of Intelligence Analysis

Intelligence analysis is defined as "the systematic collection, evaluation, analysis, integration, and dissemination, of information on criminals, especially related to their associations and their identification with criminal activity of an organized nature" (Gottlieb, Arenberg, Singh, 1994). In contrast to crime analysis, intelligence analysis deals with more serious crime types, such as organized crime, terrorism, and gang groups. The main characteristic of these crimes is that they are committed by organizations. Therefore, the common aim of both crime and intelligence analysis is to analyze the correlation between crime, criminals, and events.

As in crime analysis, criminal intelligence analysis can be classified into two broad categories, tactical analysis and strategic analysis (RCMP, 1998). In this case, tactical intelligence analysis supplies key information for strategic analysis. For this

reason, the two may overlap. Tactical analysis provides immediate applications, while strategic analysis is considered a management tool. Thus, strategic analysis is used in an ongoing effort against emerging organized crime. In addition to crime analysis, Martens (1990) states the purposes of strategic intelligence analysis, including: to identify principals and their associates within current and emerging leaders, and to supply their general descriptions and activities in certain places. Moreover, strategic analysis may be used to identify the other relationships between criminal enterprises and other jurisdictions, and to judge potential organized crime capabilities (Peterson, 1994). In addition, strategic intelligence analysis may be applied to economic, social, and governmental problems caused by criminal organizations (Schneider, 1994). Strategic intelligence may also be used to determine the structure and activities of organized crime that has penetrated legitimate business (Harris, 1976). In the view of its purposes, therefore, strategic intelligence analysis is likely to provide effective ways to make the organized crime problem more understandable. Due to the complexity of organized crime, strategic intelligence is one of the most important methods of controlling organized crime.

Both analyses focus on four aspects of criminal organizations (Fahlman, 2000):

- Capabilities
- Intentions
- Limitations
- Vulnerabilities

Godson and Williams (1998) state that using this approach in intelligence analysis produces invaluable information for policy makers, and it fill gaps in current intelligence mechanisms. This analytical approach increases the effectiveness of crime and prevention strategies in a systematic way.

Scholars and specialists have recommended making much more efficient use of intelligence in law enforcement applications against organized crime. For instance, Godfrey and Harris (1971) state that if law enforcement wants to be successful in fighting organized crime, successful applications of intelligence analysis must be achieved. Additionally, Martens (1990) emphasized the use of more systematic and rigorous techniques to understand the complexity of organized crime and to make it less mythical and more clear and scientific. Beare & Martens (1998) emphasize that the investigation and analysis of organized crime, which is more complex and sophisticated than ordinary types of crime, requires an increased importance being placed on the successful application of intelligence processes.

Martens (1990) states the purposes of strategic intelligence analysis, includes: the identification of principals and their associates within current and emerging leaders, and to supply their general descriptions and activities in certain places. Moreover, strategic analysis may be used to identify other relationships between criminal enterprises and other jurisdictions, and to judge potential organized crime capabilities (Peterson, 1998). In addition, strategic intelligence analysis may be applied to economic, social, and governmental problems caused by criminal organizations (Schneider, 1994). Strategic intelligence may also be used to determine the structure and activities of organized crime

that has penetrated legitimate business (Harris, 1976). Strategic intelligence analysis is likely to provide effective ways to decipher the organized crime problem. Due to the complexity of organized crime, strategic intelligence is one of the most important methods of controlling organized crime.

Intelligence is not a new term or tool in police tactics. However, the logic of intelligence processes is still not clearly understood by most managers (Hicks, 1998). Because intelligence use is a crucial element for effective and powerful management, the next section will focus on basic intelligence steps. Managers must have a comprehensive and scientific understanding of these steps. Although scholars explain these steps differently, the functional steps remain the same.

Information Cycle

According to Godfrey and Harris (1971), the intelligence process is achieved through five prerequisite steps as shown in figure below: collection, collation, evaluation, analysis, and dissemination. Through these mechanisms, intelligence is not limited to information found in public databases, on the Internet, or in the media; instead, intelligence is considered valuable and reliable knowledge that has been obtained through a specific process.

Schneider (1994) presents a more comprehensive intelligence process that consists of nine interrelated stages: planning, collection of information, assessment of information validity, collation of information, analysis of information, assessment of analytical rigor and value, dissemination of intelligence, application of intelligence, and the review and assessment of the criminal intelligence function or unit.

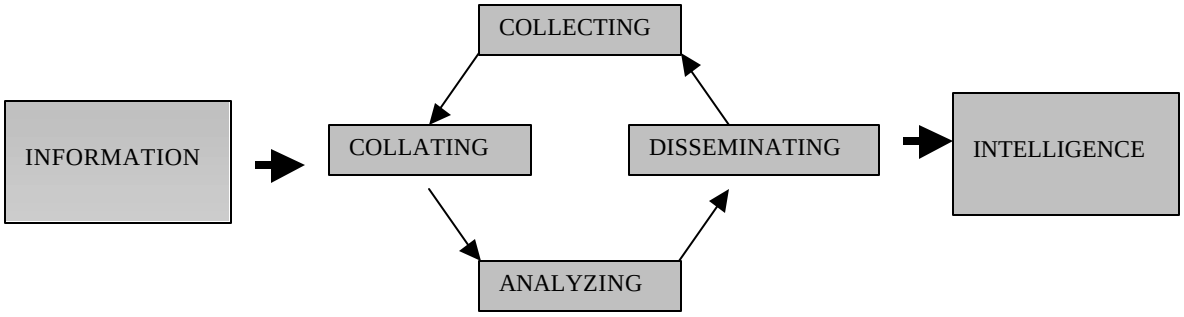

Figure 3.1. Information cycle, reprinted from: Police intelligence. (October 1999). USAMPS white paper 00-05. [On-line]. Available: http://wood.army.mil/usamps/dot/Doctrine/White%20Papers/PI.htm [June 27, 2000].

In contrast with this approach to the intelligence process, Gill (1998) tries to use cybernetic models to make sense of police intelligence. Gill defines cybernetic models as "systematic studies of communication and control in organizations of all kinds" (p.306). Because the dynamic composition of information is at the core of cybernetics, Gill argues there is a correlation between intelligence systems and cybernetics. Focusing on this point, Gill creates an analogy for the nature of intelligence. In this manner, both terms emphasize information analysis as the heart of policing (Gill, 1998). Thus, intelligence can be examined as an information system achieved through improving knowledge and controlling the environment. Overall, the experts mentioned here argue that the intelligence process should consist of a series of specific steps.

Planning

The very first step of the intelligence process is planning. Godfrey and Harris (1971) insist on the use of a directed and targeted collection system with advanced

planning. In addition, Peterson (1994) recommends that a flexible and adaptive methodology be used for the first stage of the intelligence process, thus increasing the chances of achieving the goals and objectives of an intelligence project. Schneider (1994) notes that there are four interrelated ways of planning before collection stage: conducting an environmental scan, choosing a topic for inquiry, defining the problem, and developing a collection plan. The environmental scan identifies and examines a number of crucial points, including demographic characteristics, overall crime rate, and physical conditions. In general, an intelligence unit must engage in continuous and systematic scanning of the environment in order to present its methodology.

Selecting a specific topic or crime type is the next stage. Gill (1998) argues that intelligence process cannot be successful without targeting and directing a goal or objective. This means that the narrower the topic, the more efficient and effective your search will be. Gill adds that criminal intelligence units should therefore be highly selective. Selectivity and directivity in the first stage of the intelligence process makes the process much more efficient.

After scanning the environment and choosing the specific problem, next step is to clearly define the problem. In the opinion of Dintino and Martens (1983), a strategy cannot be created until the problem is precisely defined. Therefore, the starting point in this process is to define the problem and establish a hypothesis. According to Sommers (1986), the hypothesis should then be proved or refuted by the subsequent analysis.

Finally, a collection plan that incorporates the previous planning aspects is created. In order to emphasize the importance of planning, Wolf (1978) states that

intelligence analysts must plan, direct, and coordinate the entire intelligence processes in order to avoid duplications. Dintino and Martens (1981) also support Wolf's argument by noting that a clear plan is one of the crucial stages of intelligence process. This comprehensive plan serves as a guide throughout the entire process. Martens (1990) sees the systematic planning of collection as a "road map". The intelligence process works in this specific way, from beginning to end, in a goal-oriented approach. Therefore, collection planning must be constantly reviewed and revised if necessary (Godfrey & Harris, 1971).

Collection of Information

Once planning and targeting is completed, the next step is to gather necessary information. Effective organized crime prevention is commensurate with the significance and convenience of the collected data. Hicks (1998) argues that accurate and goal-oriented intelligence can only be processed with precise and relevant information. To establish a well-defined collection effort, the problem definition must guide data collection. This allows the collection of data that is both goal-oriented and clearly relevant to the criminal activity being examined (Martens, 1987).

Suitable information should be collected from different overt and covert sources determined during the planning phase (Dintino and Martens, 1983). Overt resources include investigators, information from non-intelligence units, information from non-law enforcement agencies, and complainants. Covert resources, on the other hand, include physical surveillance, electronic surveillance, informants, and undercover agents (Godfrey & Harris, 1971). Again, Schneider (1994) argues that more the efficiency of the

collecting process depends on high quality planning and targeting. Martens (1990) recommends that information gathering should guide the search, and Gill (1998) states that the intelligence process should be directive and selective way.

Another consideration with respect to information collection is information security. Because of the massive amount of information comes from the field, informants, and other resources, it is imperative that secure and effective storage systems be used. Today, most intelligence files are saved in huge computer systems with high quality database systems such as Oracle or Access (Peterson, 1994). These types of databases are preferred because of the purpose and volume of data to be collected. From the cybernetic point of view, Gill (1998) identifies several important security issues: centralization of computers, authorization, and identification of possible sources of internal and external "resistances". Intelligence data should be computerized and stored both centrally and accessibly for intelligence department purposes. The level of authorization should be determined by the ranks of personnel working in the intelligence unit. Finally, both internal and external forces may affect the collection stage of the intelligence process. Internal resistance includes organizations attempting to contradict law enforcement efforts. External resistance includes rules, guidelines, and the diversity of authorization or security levels. In short, the collection process must consider the management and control of information sources.

Collation of Information

When information is gathered, it is evaluated within the context of the intelligence project's goals. The purpose of collation is to ascertain the reliability and validity of the

unprocessed information (Godfrey & Harris, 1971). Additionally, the information is examined to determine if it is consistent with the goals of the intelligence project, the duties of the intelligence unit, and applicable ethical standards (Schneider, 1994). This stage also ensures that the information is valuable for investigations, strategic assessments, or managerial judgments. Dintino and Martens (1983) strongly suggest that information be verified and reviewed before it is stored. Otherwise, unverified or useless data may misguide analysts. Finally, Wolf (1978) recommends that information captured from distinct resources be consistent with regard to pertinence, reliability, and accuracy.

The simple collection and storage of information is not considered 'intelligence'. Intelligence is the end product after analyzing and converting raw information into knowledge through a number of steps. Godfrey and Harris (1971) define collation as the first step of analysis. Collation of information is not limited to storage. In the collation stage, information is indexed, ordered, related, and filed in a suitable form. As a result, information unrelated to a particular intelligence project may be identified and filtered. This is why Godfrey and Harris (1971) define the collation of information as the first step in the translation of raw data into intelligence.

Analysis of Information

Most experts and scholars agree that analysis is the heart of intelligence process. Analysis is the step in which raw data is processed and converted into meaningful information (Godfrey & Harris, 1971). Individual pieces of information are assembled to create a big picture of a criminal organization's activities. In spite of its significance, the analysis stage is often not addressed as much as would be expected in police departments

(Dintino and Martens, 1983). Concentrating on this point, the analysis function of intelligence process is considered an indispensable mechanism for controlling organized crime.

There are a number of points to note about data analysis. To begin with, analysis should be conducted in two different categories, such as tactical and strategic analysis (Godfrey and Harris, 1971). Thus, administrators must assign two separate analysts to carry out this task (Dintino and Martens, 1983). This separation should depend on the size of the department. In smaller police departments, only one analyst may be available to conduct both tactical and strategic assessments. Secondly, analysts must develop hypotheses in light of the organized crime problem. The hypotheses and the problem identified in the planning stage must be considered together (Peterson, 1998). In this way, analysts should think as a social scientist. They must prove or refute hypotheses based on gathered and processed information. Godfrey and Harris (1971) strongly suggest that analysts conduct research into new trends and patterns of organized crime activities. Exploring these points, Schneider (1994) states that information analyzed in this way should be used by policy makers, administrators, and prosecutors to create new and more effective preventive policies against organized crime.

"Analysis is the key to the success of an intelligence unit," argues Harris (1976, p.18). With insufficient analytical skills, intelligence departments are essentially limited to being filing departments. The complex nature of organized crime requires the use of intelligence methods in order to predict future trends. According to Dintino and Martens (1981), decisive and logical analysis is the only mechanism that can be used to solve

organized crime problem. Randomly arresting organized crime actors is likely to increase the severity of the problem, because those arrests may aid in improving their criminal skills. This may reduce the efficiency of law enforcement with respect to allocating its limited resources effectively. Unfortunately, police agencies have not been using analysis techniques, as they should be. Analytical methods such as network analysis, financial analysis, and visual investigative analysis are considered the cornerstone of analysis stage (Peterson, 1990). Those techniques are further divided into tactical and strategic methods for controlling organized crime.

Dissemination of Intelligence

After using analytical methods to process information, the knowledge obtained should be prepared for dissemination. Schneider (1994) recommends that managers control the analytical product by focusing on the accuracy of the intelligence, well-written reports, logical flow, and rigor. This focus ensures the validity and reliability of the data before it is disseminated. Otherwise, the intelligence may misguide other agencies and policy makers struggling with organized crime.

The most important aspect of disseminating intelligence is to allocate the processed information or product to persons responsible for dealing with the organized crime problem (Godfrey and Harris, 1971). Dissemination of intelligence is such a critical stage that full responsibility should rest on managers (Gill, 1998). Management must review reports before they are distributed (Schneider, 1994). In maintaining secrecy, dissemination must be based on the principle of "need to know" (Harris, 1976).

Therefore, managers must disseminate information with regard to its level of sensitivity and confidentiality, as well as to the goals of the report.

Once disseminated, intelligence may be used by investigators, other managers, and policy makers. Each receiver must examine whether the intelligence can be applied to their respective goals (Schneider, 1994). Thus, intelligence units should try to maximize the credibility of the information that they provide. In this manner, analysts and investigators should closely work together from the first stage through the final stage (Peterson, 1997). Feedback coming from investigators can increase the efficiency of intelligence analysts. Analysts can focus on the specific points as directed by investigators so that gathered information may be more useful. In other words, the analysis is best targeted to a specific problem.

The work of the previous stages culminates in the review and assessment stage. This stage requires the evaluation of the entire intelligence study. Successful reviewing of the end product shows both the strengths and weaknesses of the results. The main objective of this stage is the periodic updating of available information. Meanwhile, applications of GIS may be useful in this stage. When the agency is considered to be insufficient or operating ineffectively, the unit administrator may address the reasons and solutions through more productive and cost-effective methods, such as GIS. Applying the above model presents an intelligence cycle which produces the end product of useable information. The analysis step in this cycle is considered most important. Analysts require specific techniques to conduct their analysis. These techniques are called analytical methods, and they are discussed below.

Analytical Methods for Intelligence Analysis

Intelligence analysis employs analytical models that detail information for tactical and strategic intelligence assessments. These techniques allow law enforcement to display complex associations, activities, and relationships in criminal organizations (Stockley, 1988). Schneider (1997) states that intelligence is the cornerstone of the decision making process for planning, organizing, and effective management of organized crime enforcement endeavors. Organized crime control units must utilize systematic techniques for the processing of intelligence. These techniques, such as link analysis and worth analysis, should be used to address organized crime activities.

Financial (Worth) Analysis

As previously mentioned, organized crime activities have entered cyberspace. Organized criminals need to launder money from illegal activities, and financial transactions among criminal organizations are how they accomplish this. Organized crime groups move into legitimate business, such as law or finance, and considering the goals of such groups, the move into legitimate business is not unexpected. Financial transactions may provide significant clues in the identification of relationships among criminals. Therefore, financial analysis or worth analysis looks at suspicious monetary transactions while utilizing particular techniques. Basic accounting techniques are involved in financial analysis tools. Balance sheets and income statements are examples of these accounting techniques.

One of the most important goals of financial analysis is to discover a net worth statement that indicates illegal earnings of individuals (Schneider, 1994). This analysis is

efficiently used in money laundering cases often related to organized crime activities. Financial analysis involves check analyses, business record analyses, as well as net worth analyses. All these factors augment the amount of information that related to organized crime (Peterson, 1998). Thus, information management and special analytical methods have an important role in handling the amount of available data.

Network (Link) Analysis

Network analysis is the "bread and butter" of intelligence units (Martens, 1986, p. 8). It consists of dissecting the internal hierarchical structure, management, and roles of individuals within criminal organizations to arrive at a complete picture of an organized crime group. Network analysis also determines and presents the linkages, associations and interactions of all known members of an organized crime group with other organized crime groups. Network analysis also addresses the operations of these groups in the jurisdiction and elsewhere. The connections and interactions between individuals and organized crime groups are referred to as the “criminal network” (Lupsha, 1980; Ianni and Reuss-Ianni, 1990; Sparrow, 1992).

Telephone Record Analysis:

Telephone record analysis is another important tool for analysts in organized crime cases. Organized criminals communicate with one another, and this is an important information source for the police. Although this method has been utilized for many years, the analytical approach has improved this technique. For instance “I2”, an intelligence analysis software program, provides law enforcement with many benefits. This software provides a representation of the patterns of all calls placed and received by organized

crime actors. An analyst can easily get the big picture of relationships in a conspiracy. According to Peterson (1998), this graphic representation of relationships is an effective tool for use in court proceedings.

Peterson (1990) presented the steps of telephone record analysis as:

1) Gather the records to be analyzed
2) Identify the scope of the calls
3) Determine the frequency of calls by date and day of the week
4) Detect the frequency of calls to specific numbers
5) Determine the length of calls
6) Identify a priority listing of frequent contacts determined in steps four and five.
7) Examine frequently called numbers for patterns
8) Review all records for geographic distribution
9) Prepare charts
10) Integrate all information above in an intelligence analysis report.

It is particularly important to analyze the geographical distribution of calls. Today, GIS tools have the capability of achieving this demand. Thus, crime and intelligence analysis methods combine at this point. Spatial analysis of calls exploits additional information to analyze the relationship between crime and geographic location.

Current Information Analysis Applications for Organized Crime

This section exemplifies recent analytical applications for organized crime and drug trafficking. The efforts discussed below are considered strategic steps in tackling

organized crime. Mapping drug trafficking trends and mapping global organized crime activities are examined to support the idea that the use of analytical methods is key in successful organized crime prevention. Geographic targeting order is discussed later, with a discussion of the use of GIS in representing monetary transactions.

Mapping Drug Trafficking Trends

The National Institute of Justice (NIJ) develops high technology to manage criminal justice information. The institute also evaluates the effectiveness of utilizing information technology for law enforcement applications. The NIJ supports law enforcement projects that are aimed at managing information. As an example of this type of project, the Pittsburgh Police Department developed a GIS model as a means of tracking drug-related offenders. The model is called the Drug Market Analysis Program (DMAP). This project emphasized intelligence-led policing through the analysis of data in terms of geographic criteria. This strategic approach was considered much more effective than the use of basic, street level policing.

DMAP is one of the most important policing efforts in combining GIS and various law enforcement information. It is currently used for narcotics enforcement. In recent years, this project has been expanded to a map-based crime analysis system through the use of complicated statistical methods. The new version of DMAP has many purposes, including criminal investigation. For instance, DMAP may easily allow detectives to find highly detailed information about specific geographic points. Another, purpose is to allow law enforcement officials to measure the efficiency of policing efforts by examining the geographic movement of crime with respect to time and place. These

parameters may be designated via GIS maps that show the spaces of units. For court representations, DMPA allows law enforcement to present graphic evidence of criminal relationships.

The information gathered from DMA P has contributed most to research in drug-related cases. For instance, Olligschlager (1997) improved a spatial tool for street level drug markets. The main purpose of his study is to track street-level drug markets and to offer an artificial intelligence-based GIS model as an early warning system. Briefly, these applications provide evidence that GIS mapping systems are important managerial and decision making tools for law enforcement efforts.

Mapping Global Organized Crime Activities

Organized crime groups have changed with respect to size and their range of activities. These groups are now an international threat to most countries. The reason is that criminal organizations have formed global networks to effectively accomplish their activities. Today, criminal organizations, such as the Italian mafia, Russian mafia, and Chinese organized crime groups may integrate their activities to increase profits. As a result, they are likely to move into the financial, economic and political areas in countries all over the world. This idea is supported by many researchers, such as Albanese (2000), Abadinsky (1997), and Levi (1998). For this reason, international law enforcement efforts must be activated to address this problem.

In recent years, international law enforcement agencies have been involved in particular projects for organized crime prevention. One of the most significant projects involves the mapping of transnational organized crime activities (UN, 1999). The

primary objective of this project is to provide member states and the international community with reliable information and analyses of the emergent trends in organized crime activities. This project also ranks transnational organized crime groups according to their level of dangerousness. The designation of a level is based on various characteristics of criminal organizations. Forecasting of future trends of criminal organizations is another goal of this project. Using this information, law enforcement agencies may establish strategic plans and programs to address the organized crime issue.

When the mapping of transnational organized crime groups is established with GIS technology, the flow of information will allow the project to develop dynamic maps. Such a dynamic mapping system would contribute to agencies' understanding of the dynamic attributes and structures of transnational crime syndicates. Using such a sophisticated technology will lead to the establishment of descriptive and static maps to combat organized crime. Consequently, these maps may allow law enforcement agencies to freely share their information with one another. Agencies establish their own maps, and these maps may be compared with maps from other agencies to determine emergent trends at both national and international levels. In short, this project aims to depict the movements of dynamic organized crime activities all over the world. As previously mentioned, using the graphic information from GIS applications also leads to the more efficient and effective use of resources for all agencies using the information.

Regional Information Sharing Systems

In the U.S., Regional Information Sharing Systems (RISS) aim to support federal, state, and local law enforcement efforts against criminal activity across jurisdictional

boundaries. The primary focus of RISS is organized crime and drug trafficking activities. More than 300 state agencies and more than 600 Federal agencies participate in this systems (Gist, 1998). This system consists of the following six regional projects:

- MOCIC (Mid-States Organized Crime Information Center)
- MAGLOCLEN (Middle Atlantic-Great Lakes Organized Crime Law Enforcement Network)
- NESIN (New England State Police Information Network)
- ROCIC (Regional Organized Crime Information Center)
- RMIN (Rocky Mountain Information Network).

Each regional RISS center can communicate with other centers via secure intranet, electronic mail, telephone, fax, or person to person. Intelligence and analytical personnel have an important role in managing the information flowing from the numerous resources. The two main aims in these programs are information sharing and data analysis. Information sharing governs input and dissemination, expeditious retrieval, and methodical upgrading of criminal intelligence. Data analysis focuses on telephone toll analysis, financial analysis, information sharing, and other data analysis techniques. Briefly, RISS allows gathered information to be analyzed through specific analytical methods. RISS also provides quick and secure information sharing among law enforcement agencies. Therefore, it is considered an effective program in the prevention of multi-jurisdictional crimes, such as organized crime.

This program may also be used to foster information sharing within centralized police organizations. Decentralized organizations may be unified through the use of a

program such as RISS, and this may lead to the more efficient exchange of internal information.

Geographic Targeting Order

In this section, the use of Geographic Targeting Order (GTO) is discussed, and its uses for money laundering operations are presented. GTO, as a means of money laundering investigation, examines the high dense money transactions in financial institutions (Evans, 1997). Money laundering is one of the most important activities of criminal organizations. It is defined as a series of multiple transactions utilized to disguise the true source of funds (Manning, 1999). The International Narcotics Control Strategy Report (1998) presents the money laundering process as having three different elements including placement, layering, and integration. The process of money laundering is generally achieved through these steps. Placement involves depositing currency in a financial institution. Layering is the process of shifting money from one institution to another to "hide" the funds. Then the funds are invested in legitimate business during the integration phase.

The GIS model may be used in conjunction with GTO to examine financial transactions in money laundering investigations. Financial services may include money transmitters, traveler's checks and money order issuers and sellers, retail currency exchangers, and check cashers (Richards, 1999). The coordinate information of financial institutions is entered into GIS maps. As applied in drug cases, GIS may be used to analyze the trends and patterns of money transactions for strategic purposes. According to International Narcotics Control Strategy Report (1998), many suspicious transactions

may occur in small cities. The activity should be noticeable in that the volume of transactions in the city is higher than expected. GIS has the ability to represent all transactions with respect to place and amount. Using this data with GTO may provide law enforcement with incredible benefits in examining the relationships between criminal organizations.

Conclusion

This chapter examined the crime and intelligence analysis techniques as information analysis tools for law enforcement efforts. It is suggested that crime and intelligence analysis be handled together for successful organized crime prevention. The logical steps used to analyze information, in each case, is the same. The only difference between crime and intelligence analysis is that intelligent analysis looks at relationships within and among criminal organizations, and crime analysis deals with trends and patterns of criminal activities. Overall, this chapter stressed the importance of CIA (Crime and Intelligence Analysis) for successful organized crime prevention. GIS and information management are considered as essential weapons for local, national, and international efforts against organized crime.

CHAPTER IV

ANALYSIS OF PROBLEMS FOR INFORMATION ANALYSIS

Introduction

In previous chapters, the shift in organized crime activities has been stressed, and the integration of crime and intelligence analysis has been suggested for preventing the organized crime problem. The suggestion was based on the idea that proactive approaches are much more effective and efficient than reactive approaches. Proactive policing is not related to arrest rates, but it emphasizes prediction and prevention (Taylor, 1987). In advocating for proactive policing, analytical tools covering both crime and intelligence analysis have been stressed to provide law enforcement with information management at national and international levels. However, utilizing these powerful analyses in organized crime prevention leads to critical issues in practice.

Peterson (1998) emphasized that law enforcement has not been successful in the implementation of intelligence and analysis techniques in combating organized crime. She indicates three reasons for the lack of successful usage. One of the main reasons is that analysts have fallen short in expressing the benefits of intelligence and analysis to managers in the unit. Second, managers have not been able to successfully exploit the applications of analysis because they have been reluctant to diverge from traditional investigative techniques. Another reason why law enforcement units are reluctant to utilize analysis function is because of the cost involved. The software programs required to perform these tasks may be too expensive for many units. Another related issue is that

researchers and practitioners do not receive professional recognition or support for their crime and intelligence analyses.

This chapter focuses on the problems and issues with information analysis. These problems and issues are examined as: technological issues, managerial issues, and privacy issues. Technological issues include both high costs and difficulties in handling sophisticated technology. Managerial issues include the lack of understanding by managers, and the relationships between analysts and officers. Privacy issues include the issue of invasion of personal rights due to the misuse of crime and intelligence analysis methods.

Technological Issues

Crime and intelligence analysis is a process that requires computer technology. Both pattern and link analyses may not be accomplished without special software and hardware. Therefore, technology has played a critical role in the application of analysis tools. It has allowed law enforcement to work more intelligently and efficiently. However, many issues and concerns appear when information technology is need in criminal analysis. Rich (1995) notes several barriers in the use of technology as a crime analysis tool. These barriers include hardware and software costs, expertise, data acquisition costs, network costs, and data quality. These issues are addressed below.

Cost Issues

Dunworth (2000) notes that most of the costs associated with computers and their use have declined as desktop computers are used frequently in daily life. Consequently, crime analysis has grown thanks inexpensive computer technology. Sophisticated PC-

based mapping software packages (Arc View, MapInfo etc.) have all contributed to the improvement of crime analysis. Although the cost of high technology has decreased, some barriers may still exist in utilizing analysis tools. In fact, most agencies have been reluctant to use crime and intelligence analysis tools (Fahlman, 2001). As the amount of information increases, law enforcement must handle much more sophisticated information management systems and network technology. These systems cost more than personal computers. Particularly, huge database systems and their servers may be very expensive. This means that the costs of technology are still prohibitive.

Hardware and software costs seem so high that mapping software starts with a few thousands dollars (Rich, 1995). Particularly, "i2" intelligence analysis software costs more than 5,000 dollars (Fahlman, 2001). If this software is used on multiple computers or as part of an "intranet, "the cost may be higher. Therefore, most agencies heavily weigh the costs of information technology before stepping into the technologically supported crime analysis environment.

There are also financial benefits in this technology. About 554,000 police officers serve in local and state police agencies (Feldman, 2001). Information technology may serve to reduce the number of required personnel in a law enforcement environment. When one compares personnel salaries with the cost of technology, the cost of technology is not so much higher than the total cost of employees' salaries. Further, information technology contributes to more efficient law enforcement work. Agencies must determine the level of information technology use appropriate to each agency's

budget, missions, and goals. There are many factors to consider in both large and small law enforcement agencies.

Expertise

Sophisticated technologies require skilled personnel who are able to utilize sophisticated software programs, such as i2, Arc view, MapInfo, and, Arc Info. Unfortunately, the expense of training these persons is considerably high, and this has led to reluctance on the part of law enforcement to use technical tools. This point also makes law enforcement reluctant to handle analysis tools.

Data Quality

Another problem related to technological aspects is the quality of data for analysis. As mentioned earlier, open sources and other useful sources including police and court records have increased the flow of information into the law enforcement environment. The issue is how the agencies select data relevant to the goals of the agency. Not all information will be valid to use, and the data must also be checked for reliability. If the information is not fully realized, is not precise, or is not gathered in a timely manner, the analyses are less valuable. At worst, the results obtained from such information may result in incorrect assessments about organized crime. Assessments based on inaccurate data may misguide policy and decision makers. Indeed, this is not only expected in law enforcement environment

Privacy Issues

As information technology develops, more and more information about individuals will be stored in police intelligence databases. In fact, this is one of the most

significant exercises of intelligence units. Security becomes a serious issue at this point. When information is recorded in paper-based methods, possible access from outside may be restricted. Intelligence units do not disseminate personal information without having a reasonable demand. In case of digitally stored information, it may be easier to transfer digitalized information from one place to another. Because of this, it is imperative to have effective security measures in place to control this information. These controls include "need to know" principle, data security, and secure data transfers.

Law enforcement officials must be aware of the possibility of unauthorized access to information. Insiders and outsiders are likely to access the database, sometimes without leaving any trace (Dunworth, 2000). Unauthorized access may lead to destructive abuses. For instance, organized crime groups hire hackers to steal law enforcement information from its databases (Technology and Crime, 2000). Security issues may result in limitations to the amount and type of information used and stored for organized crime policing. This restricts the capability of information technology and its users. Consequently, future developments in information technology must address and establish protections for individual privacy as well as the advantages for law enforcement applications.

The prevention of organized crime requires data related to individual persons, families, or households. The police may access and compile this data for the purpose of investigation in a network system. For instance, monitoring credit card information allows law enforcement to track the purchases of suspected criminals (Harries, 1998). When this information is added to a GIS database, analysts may track the geographical

places where criminals act. This information may also be integrated with satellite images and aerial photos. In short, various forms of information may be combined together for information analysis.

As the implementation of open sources (i.e. information on the Internet) and sharing capabilities increases between information systems, personal information is more likely to be involved and transferred in these systems. For this reason, justice leaders are increasingly being compelled to examine and address information privacy issues (USDOJ, 2000).

In organized crime prevention, law enforcement handles sophisticated technology, including huge databases, crime maps, and computer network systems. Information management is a requirement for the success in fighting global organized crime. However, there is a question as to whether the police have used information technology in proper way or not. On one side, the police have to utilize this technology to identify criminal activities. On the other side, people have reasonable expectations for their privacy.

The meaning of "privacy" includes values, rights, and interests that are particular to the individuals (Zoufal, 2000). Privacy includes privacy of the person, privacy of personal behavior, privacy of personal communications, and privacy of personal data. The final term is also referred to as information privacy. This section addresses the issue of information privacy and security.

Privacy is more likely to be invaded in information gathering phase. In integrating and analyzing the information, there may be less of a threat. Analysis is

essential for identifying criminal activities. This critical point requires that law enforcement ensure the consistency between data, the mission of intelligence agency, management policy, and ethical issues (Schneider, 1994). Failing to consider this may result in serious privacy issues.

Accordingly, information privacy is ongoing concern among law enforcement officials and the public. The reluctance to address privacy problems related to information management systems may lead to detrimental effects. The public is likely to be afraid that their personal information enclosed in law enforcement files may be accessible or releasable for third parties. Accessibility to this information may result in loss of employment or social status for the reason whose information was obtained (USDOJ, 2000). The public becomes subject to the risk that their information may be falsely linked to the name of a criminal.

The lack of concern about privacy issues may also be destructive to law enforcement agencies. Agencies may spend billions of dollars on information systems to improve the effectiveness of analysis. These systems may allow law enforcement to eliminate duplication of effort, delays in the dissemination of information, and obstacles to accessing information. Further, information systems may assist law enforcement agencies in scheduling and case management

If agencies are reluctant to assess the possible public privacy effects, their effective and efficient multi-million dollar information management systems may be useless. Therefore, public policies are necessary to protect both privacy and the technology investment. Personal privacy may also be invaded in bankruptcy cases for

possible money laundering investigation (Bernstein, 2000). In these cases, police and other responsible agencies may wish to gather highly sensitive personal information, including social security numbers, financial information, credit information, income, and details about routine living expenses. Data collected for such cases are likely to invade the individual privacy.

Managerial Issues

Management has always had an important role in public services. An environment where massive amounts of information are analyzed and stored by means of sophisticated technology requires effective management. Intelligently managing technology and its users provides a pivotal force for developing crime and intelligence analysis. The philosophy of management must be to establish an environment that is conducive to effective intelligence processes.

Analyst versus Officer

The managers of information analysts must establish proper relationships between analysts and police investigators. The lack of positive relations may result in critical problems. Indeed, both analysts and investigators are essential for successful organized crime intelligence efforts. Schneider (1994) notes that managers are responsible for encouraging interaction and continuous dialog between intelligence analysis and operational personnel. While analysts are able to synthesize data coming from the field, a well skilled investigator is imperative to provide the flow of continuous information. Therefore, these two persons cannot be considered separately. Considering the issue, team policing is meant to prevent the inconsistencies between analysts and investigators.

Team policing gives equal importance to every person whether they are performing the investigation in the field or analyzing information in a computer. All persons are intended, therefore, to work together in team policing.

Analysts attempt to gather all data that are necessary for the analysis. As cited in Goodwin (2000, p.1), Stoneman notes that analysts typically spend their time “trying to get the data together rather than analyzing it." This exemplifies the lack of success in management.

Analyst Recruitment and Training

Crime and intelligence analysis requires specifically trained and highly skilled analysts. For this reason, the recruitment and training of analysts plays a significant role in achieving the logical steps of CIA. Staffing the analysis unit requires a lot of attention. The unit must include specialized, and critically thinking analysts.

Beare and Martens (1998) argue that the importance of analysts should increase as high technology develops. However, some managers consider it unnecessary to hire analysts because sophisticated and user-friendly programs are able to achieve everything. Unfortunately, as Dunworth (2000) notes, technology cannot do anything without skillful users. The proper processing and analyzing of information requires knowledgeable analysts. Further, these analysts must be trained with highly sophisticated training courses.

Analysts must also have sufficient knowledge of theories of organized crime, research methodology, and policy analysis (Schneider, 1994). Analysts must also have the ability to develop analytical techniques. This is a particular skill necessary to be an

analyst. Therefore, the manager of a crime analysis unit must pay particular attention in recruiting analysts. This may limit the number of possible candidates, because an analyst must have background knowledge about organized crime theory. This point makes it difficult to hire analysts who are well experienced in organized crime policing.

Conclusion

This chapter addressed the problems and issues for information analysis in law enforcement. These barriers were classified into three distinct issues, including technological issues, privacy issues, and managerial issues. It was argued that law enforcement must balance benefits of the information with privacy concerns. Ultimately, privacy barriers may result in dire consequences. For instance, it may restrict the development of information systems because they are likely to victimize innocent people. The issue of cooperation was addressed. If managers are not successful in establishing consistent relationships between analysts and investigators, the full effect of CIA may never be realized in the fight against organized crime. Therefore, it was expressed that management must play a key role in ensuring the issues mentioned are addressed appropriately and effectively. The next chapter addresses solutions to the above mentioned problems including ways management may rectify the issues.

CHAPTER V

ANALYSIS OF SOLUTIONS FOR INFORMATION ANALYSIS

Introduction

Information analysis renders many benefits to law enforcement regarding the prevention and investigation of organized crime. Nevertheless, it has been argued that law enforcement has faced particular problems in handling information systems. These problems include the inefficient use of information technology, the risks of privacy invasion, and ineffective management of analysis units. It is imperative that governmental and other institutions address these problems with information analysis. From the time when information analysis was first used, many solutions have been offered for these problems. Although the solutions may be distinctive in terms of the size of police units, this chapter highlights solutions for information analysis with regard to organized crime activities. Therefore, the solutions are examined under following headings: managing information and technology, privacy issues, educational issues, sharing among international organizations, and managerial issues.

Managing Information Technology

Combined crime and intelligence analysis may not be achieved without the use of technology. New systems and techniques are emerging to make analyses more effective and efficient. However, tracking new technology may be costly. Besides the costs of information technology, law enforcement agencies must also consider the costs of training courses which must be provided to personnel. Due to the fact that high

technology may be very expensive, agencies must take care to get the maximum benefit from it. This requires the management of technology. The objective of technology management is mainly to meet the expectations and goals of an agency engaged in a high tech enterprise. This section addresses particular solutions in handling information technology as it applies to organized crime detection and prevention.

Choosing Appropriate Equipment

Technology has been changing rapidly. Hardware and software are considered essential in conducting information analysis. Further, technology may also refer to an interface with an information management system that contributes to law enforcement data query and download capabilities. The number of information systems available today may cause difficulties in selecting appropriate technology, such as analytical software. Examples of analytical products include: Arc Info, MapInfo, and I2. Each software has its own powerful characteristics, including the number of information layers (similar to tables in other database systems), technical support after purchasing, and the compatibility with other database systems. It is difficult to articulate which one is the best in and of itself, but the choice should be based on the objectives and the mission of the particular agency. If the objective of the agency is to disseminate information via e-mail or to publish maps on an intranet, it is imperative to utilize a HTML-based program. This process is also referred to as a retrieval design of information. Most software, such as PERL, allows the downloading of HTML programs. PERL is a web client program that retrieves information with a web server (Wong, 1997). Overall, the choice made must be consistent with the needs assessments conducted for the agency.

Assessments for needs relating to crime and intelligence analysis directly relate to how analytical products are currently used in the agency. For this reason, Boba (2000) offers a guideline for assessing the needs for an analysis unit. The assessment must be closely coordinated with the requirements and the amount of money available for technology. Conducting a needs assessment is considered a basic issue in the management of information technology. Managers must determine costs, the data being collected, how the intelligence is being produced and disseminated, and who is gathering, producing and distributing the information.

The effective and efficient selection of information systems is directly related to the knowledge about the information process. Police agencies have already been using spreadsheet programs (such as Excel) to establish the tables indicating crime patterns and trends. Spreadsheets are not considered sophisticated or efficient methods of data representation, but the use of spreadsheets exemplifies the logic of police intelligence processes.

As mentioned, the processing of information using objective factors includes the use of strategic goals, data sources, technology, and the characteristics of crime and intelligence analysis. However, if this information is not integrated with subjective information, and is not synthesized in the assessment of the information analysis needs of the agency, objective information will not provide the most accurate assessment of need. Boba (2000) posits two different methods of obtaining subjective information, formal and informal way. Formal method requires a committee of individuals to determine the needs of an analytical unit. The informal route includes a set of questions presented to the units'

analysts. This is a type of interview presented directly to analysis staff. Although both methods may be time consuming, each has a significant role in deciding which information technology is more suitable to the objectives and the mission of the agency. At this point, analysts are considered the most eligible persons to produce new insights and perspectives in developing crime and intelligence analysis systems.

Preparing Guidelines

It is evident that sophisticated technology and its products are the heart of crime and intelligence analysis. Implementing crime and intelligence analysis through this technology requires particular steps, including the identification of goals and objectives, determining the type of information technology to be utilized, recruiting analysts, and utilization of analytical software. If law enforcement agencies develop proper procedures to accomplish the process of information analysis and to handle its required products, it may actually increase overall effectiveness and efficiency of managerial efforts. Considering this, law enforcement agencies must spend the time to prepare appropriate guidelines for analytical units. Boba (2000) presents a comprehensive guideline to implement and evaluate crime analysis and mapping in law enforcement agencies. This guideline includes the following steps: assessing the crime analysis and mapping needs of the agency, developing an action plan, and the evaluation of crime analysis and mapping efforts. Then, these steps are analyzed in terms of personnel, technology, data sources current and future needs of the analytical unit, training, and promotion. This guideline presents a dynamic process through which a crime analysis unit is developed and maintained.

Designing WEB Page

Today, people are increasingly using the Internet to learn about and distribute information on a variety of topics. Internet tools also have an important role in law enforcement applications for the information retrieval design. The standards and essential steps in implementing analysis methods may be disseminated through a web page. Majority of police departments and intelligence units have their own web pages. Regarding the significance of information and experience sharing, web page applications are likely to contribute the dissemination information and new developments in crime and intelligence analysis. Further, web pages may provide agencies with the ability retrieve departmental information, including periodic bulletins, statistical data, crime maps, and advertisements for personnel recruitment. Nevertheless, the amount of available data and its level of confidentiality must be considered. In short, the efforts in information and technology management may be augmented through the use of web pages.

Global Justice Information Network

Information networks have been used for technology management in the U.S. since the very first efforts in information management. Indeed, law enforcement agencies are expected to share their information related to organized crime activities that are likely to be threats to local, national, or international security. Considering the flow of vast amounts of information, agencies must be managing this information by using sophisticated network and database systems. One of these systems, the Global Justice Information Network (GJIN), aims to enhance effective and efficient use of information technology and criminal intelligence among law enforcement agencies (GJIN, 2000).

Another objective of this network is to implement and evaluate standards of information exchange between agencies. Currently, many agencies have their own network system used to retrieve information. Most of these networks utilize the Internet to connect the agencies' network systems. Using the Internet allows for broader information sharing among local, national, and international agencies. More importantly, as new technologies are enhanced for Internet-based applications, this global network allows law enforcement agencies to quickly upgrade the current software. Further, this new network system allows new users into the system, thus expanding the amount of available information. These characteristics make the GJIN a global system.

The existence of a secure environment is the main issue considering the flow of information (GJIN, 2000). Today, organized crime groups are hiring hackers to access and steal law enforcement records (Technology and Crime, 2000). Consequently, although internet technologies provide many advantages to law enforcement efforts, agencies must consider the security of exchanging intelligence via Internet. Regarding security, Denning & Baugh (1997) examined the characteristics of encryption in law enforcement applications. The purpose of encryption is to convert 'plaintext' into 'cipher text' (Froomkin, 1996). Decryption refers to any process to convert 'cipher text' into 'plaintext'. Despite the advantages of encryption, Denning & Baugh (1997) argues that encryption security regulations and laws allow encryption methods to be disseminated to private users. She adds that organized crime groups exploit the benefits of encryption to make their own communications secure and inaccessible to others. This makes trail of organized crime activities harder to follow. In short, encryption must be the focal point of

exchanging law enforcement information via Internet. Law enforcement must consider the use of encryption methods, and must determine the level of encryption required for their operations.

Privacy Issues

Proper regulations and laws are necessary to handle the problems coming from possible gaps between reasonable expectations for information privacy and advancing the process of crime and intelligence analysis. This section considers ethical standards and privacy impact assessments to regulate processes included in information gathering and its dissemination.

The ethics of information collection is a serious legal issue. According to the International Association of Chiefs of Police, standardization in recording legal information must be the focal point in the prevention of privacy invasion and misuse of law enforcement data (Schneider, 1994). Standardization provides particular rules and limitations on gathering information for crime and intelligence analysis.

Organized crime prevention requires communication among databases of justice agencies, including law enforcement, prosecution, defense, courts, corrections, probation, and parole. Communication should also be expanded to include other agencies, such as education, health, social services, and transportation. These databases consist of individual records; therefore, the rise in sharing information for combating crime has resulted in new period in privacy policy (USDOJ, 2000). The Privacy Impact Assessment (PIA) aims to identify privacy concerns related to information access, information

gathering, information use, storage of information, and retrieval of information throughout the entire justice information systems (PIA Guidelines, 1999).

The process of PIA requires particular steps to accomplish the above goals. The process consists of the following:

1. Mapping the flow information or data from various resources.
2. Analyzing the information and data flow to monitor the consistency between information practices and relevant statutory requirements, and to monitor for compliance with relevant statutory requirements.
3. Analyzing privacy issues by means of risk assessments.

Mapping information in privacy assessments is considered a useful component in determining information decision points and privacy vulnerabilities. Besides the consistency between privacy analysis and regulations, PIA examines whether current policies and laws can meet the desired privacy protection.

Combining the methods and strategies to protect the personal privacy appears to be the most effective method. For instance, in Canada, there are important methods used to maintain privacy, including the implementation of fair information practices, privacy-enhancing technologies, privacy impact assessments, standards, and public education (Information Industry Association, 2001). FIPs (Fair Information Practices) specifically address the retrieval of personal information. The guideline for FIP states some common principles for FIP, including:

- Establishing public awareness and openness of information policies and practices.
- Providing relevant and necessary information.

- Establishing the proper use of information in advance.
- Recognizing the responsible person for privacy protection in an organization.
- Getting confirmation from the person to disseminate his/her personal information.
- Keeping individual records accurate and complete.

Privacy Enhancing Technologies (PETs) have been improved to assist in the protection of privacy (Goldberg at.al, 2001). For instance, encryption and digital signatures may prevent privacy invasion. Both techniques provide individuals with the ability to maintain and protect their personal records. As suggested, if technology is handled properly, it provides effective solutions for law enforcement efforts while maintaining individual privacy.

In short, while law enforcement agencies are exploiting the opportunities of information systems, they must consider threats to privacy. The approach outlined above requires standard rules and methods to protect privacy. There must be consistency between privacy concerns and the use of information systems. Regulations must protect the privacy rights without hindering legal efforts. Otherwise, organized criminals may use weakness a inconsistencies to their advantage.

Educational Issues

The complexity of analytical methods requires high level of education. Stallo (1995) claims that proper training programs to educate analysts may require between two weeks and seven months. In training sessions, there are two important approaches in dealing with analytical techniques. One is to use proper and effective software programs to facilitate data evaluation. The other approach applies to developing and improving

analysis techniques. This refers to research and development centers. Analytical programs, such as I2, Arc View, and MapInfo, may be learned in training courses. The improvement of analysis techniques requires experts in analysis and computer programming. Again, education is key for effective and efficient data analysis.

As intelligence-led policing is increasingly performed by law enforcement agencies, the curriculum for police education must be modified to address the developments in information systems. Besides the theoretical framework on organized crime, the prevention strategies thought must address the academic importance of crime and intelligence analysis. To combine the analysis and academic environment, Prunckun (1996) explores the relationships between law enforcement intelligence process and social search. In fact, both follow the same steps to achieve their goals. While social research deals with a topic or question, intelligence analysis focuses on a target. The target may include organized crime. As social research and intelligence processes are related, universities and colleges should present new curriculums to assist law enforcement in handling obstacles in applying crime and intelligence analysis. Information processes are frequently and increasingly applied in law enforcement; therefore, analytical techniques must become the backbone of the criminal justice curriculum.

The International Association of Law Enforcement Intelligence Analysts (IALEIA) (2001) explains that only some universities and colleges present the available programs for crime and intelligence analysis. The universities providing this information are Michigan State, Northeast Missouri State, California State at Fullerton, and

Mercyhurst in Pennsylvania. Some universities in Australia offer a special curriculum for analysis as an integral part of criminal justice education (Peterson, 1997).

The Mercyhurst program presents a curriculum that focuses on research and intelligence analysis. The courses scheduled in this curriculum include a research analysis integrating seminar, research methods and analysis, and a research/intelligence internship. This program provides BA degree with the major of research and analysis.

California State at Fullerton provides a crime analysis course in its criminal justice curriculum. This course aims to examine the relationship between crime analysis units, field and investigative operations, and administrative units as well as the process of how crime analysis is conducted. Additionally, this university provides certification programs for the professional recognition of crime and intelligence analysis in criminal justice world. The recognition of information analysis has a significant role to be enhanced and widely used. This certification program allows persons to work as an analyst.

The Queensland University of Technology in Australia includes a program concentrating on criminal justice analysis and private security. This program consists of intelligence process theory and application, police intelligence issues, protective security, and automated information systems (Chantler and Wigan, 1993). This university provides undergraduate and graduate level programs in intelligence and security.

Peterson (1997) notes that academic research concepts and applied analytical techniques may be combined as a unit of study. She offers many ways to accomplish this integration. For instance, students may be assigned to analyze various information by

means of analytical methods, including mapping software, and other intelligence analysis techniques. Another method is to invite practitioners into the class as guest speakers. These experts show students how to handle analytical techniques in practice. Team teaching is considered another alternative integrating academic topics and analysis. This method requires close coordination between professors and practitioners. This teaching model is considered best way because it brings field experience into the class. Alternatively, analytical techniques may be demonstrated in organized crime classes. As previously stated, these analytical techniques are all tools used to investigate and track organized crime activities. Considering the relationship, it makes sense to teach applied law enforcement analysis in an organized crime focused course.

In short, there is a close relationship between social research methods and intelligence analysis. Originally, Godfrey and Harris (1971) merged social research methods with law enforcement intelligence processes. Since the very first use of intelligence analysis, many analytical methods have been improved for combating organized crime. Therefore, these inseparable methods must be combined in a new criminal justice curriculum.

Sharing among International organizations

This section addresses the significant role of the International Association of Crime Analysts and other organizations in the process of sharing analytical techniques and networking information systems. Because many techniques are necessary to analyze data related to organized crime activities, it is essential to share information and experiences at local, national, and international level. This also allows analysts to track new

developments in the realm of analysis. For this purpose, the Internet is considered the best way of transferring information. In considering the above issues, the International Association of Crime Analysts (IACA) and International Association of Law Enforcement Intelligence Analysts (IALEIA) are examined in the following sections.

International Association of Crime Analysts

Implementing crime and intelligence analysis requires solid relationship between analysts, managers, and other personnel responsible for the analysis of organized crime. This inseparable relation is imperative for success in improving decision-making process and prevention policies for organized crime. An international organization is the requirement to share information and experience regarding the analysis of organized crime. This perception is consistent with the changing nature of organized crime. As previously stated, organized crime transcends the international boundaries (Albanese, 2000). Law enforcement must relate to one another at the local, national, and international level. The IACA has the responsibility for establishing a coherent relationship among police chiefs, police officers, detectives, crime and intelligence analysis personnel, and other persons who are likely to be interested in tracking law enforcement data (IACA, 2001).

IACA facilitates information and experience exchange among members regardless of their location. The members of IACA range from police officers to academic persons. This organization prepares a suitable environment to integrate the field and academic perceptions on crime and intelligence analysis. Further, IACA aims to present standards for analytical techniques and to schedule proper training courses In

short, IACA aims to enhance communication among individuals and the law enforcement agencies in the world.

International Association of Law Enforcement Intelligence Analysts

The number of academic studies on law enforcement analysis has increased in the last two decades. Specific journals on analysis have been published throughout the development of information analysis in law enforcement. For instance, International Association of Law Enforcement Intelligence Analysts (IALEIA) publishes the "IALEIA Journal" which discusses the developments of crime and intelligence analysis in relation to organized crime (Peterson, 1997).

The purpose of IALEIA is to enhance proper standards of professionalism for intelligence analysis all over the world. This association aims to improve intelligence analysis with the following objectives.

- Support intelligence analysis as a professional career.
- Advance international qualification and competence standards for analysts.
- Design training standards and curricula.
- Schedule research projects on intelligence analysis.
- Retrieve ideas and experiences relating to intelligence analysis (IALEIA, 2001).

Crime Mapping Research Center

GIS technology has grown dramatically as a means of powerful analytical tool in law enforcement analysis. This development requires academic research on the technology. The Crime and Mapping Research Center (CMRC) is one of the largest organizations to improve crime mapping and analysis technology. This group promotes advancement of

computerized crime mapping and its products. Its contribution on improving crime mapping may be examined in the concerns, including research, evaluation, development, and dissemination. In the view of these concerns, the CMRC encourages analysts to do research while providing fellowship. Further, it evaluates the current practices of crime mapping in agencies. It allows the analysts to take courses in establishing crime maps with GIS and in tracking developments. Finally, CMRC disseminates relevant information and research through conferences, and web pages (CMRC, 2001). Overall, this section emphasized the significant role of international organizations in sharing information and experience. Sharing information among the analysts allow them to work more efficiently all over the world.

Managerial Issues

Analytical units and their management are necessarily interrelated. Basically, analytical methods require skilled managers to make effective and efficient decisions in the units. Specifically, GIS allows the police management to effectively deploy all law enforcement resources. Although GIS and other analytical methods provide managers with powerful tools, managers must consider many things.

The effective and efficient use of information analysis directly relates to how managers of analytical units organize the working environment. In other words, management has a direct impact on the success of analysts. Managing analysts who deal with organized crime issues is much more difficult than with other types of crime. This difficulty stems from the vast amounts of information associated with the complex nature of organized crime activities. This section outlines methods to assist managers of

analytical units. These methods are examined with a focus on promoting research, training, and recruitment.

Supporting Research

Management must support research efforts to improve methods of information analysis. Heuer (1999) stresses the importance of cognitive processes to make intelligence judgments more effective. Therefore, analytical unit management must determine how to train analysts to improve these skills. Having these skills encourages analysts to comprehend intelligence processes more universally. Analysts that deal with organized crime investigation must have extensive analytical skill and must conduct research on improving analytical methods.

Recruitment of Analysts

Selecting analysts is a very controversial issue. Peterson (1997) states that analysts must have the appropriate academic background in order to perform analytical methods. In contrast, Dintino and Martens (1981) claim that analysts should be recruited from current personnel employed by the police department. Managers must decide whether to hire civilian or officers.

Because analysts have such an important role, managers must prepare comprehensive selection criteria. Prunckun (1990) notes there are many problems with using subjective criteria for the selection of analysts. He indicates that the quality of analysis may be lower when performed by subjectively chosen analysts. Schneider (1994) posits a diverse range of criteria in selecting analysts. According to him, analysts must have a strong background, including technical, social scientific, computer, and police

operational experience. Further, an analyst must fully understand organized crime theory, research methodology, and policy analysis (Martens, 1987).

Frost (1985) lists the essential characteristics of an analyst. Although it is difficult to choose an analyst using only these criteria, these attributes should be taken into consideration. These attributes are:

- Intellectual curiosity.
- Research ability.
- Previous experience.
- Willingness and capacity to make judgments.
- Writing ability and self-direction.
- Skill in oral briefing.

Previous experience is considered an important attribute for an analyst, but other characteristics must also be considered. In short, recruitment of analysts is an important and controversial issue. Regardless of whether the recruit is an officer or a civilian, he or she must be at least curious about analyzing information. Such persons may be properly educated by more experienced analysts currently employed in the unit.

Training

Although training is a very important issue to consider, a full explanation of this topic is beyond the scope of this paper. This section considers the training of organized crime information analysts. One of the first steps is deciding the level of training. This refers the consistency between the mission of the unit and the required degree of training. Boba (2000) advises managers to identify their priorities before determining the

appropriate training for staff. It may not be necessary to have all analysts take an outside analysis course. Training courses may cost as much as $ 5,000 per each person (MapInfo, 2001). The departmental budget may not allow for this. It may be more feasible to send one or two persons to training on such sophisticated analytical techniques, such as the use of the GIS mapping system. Nevertheless, managers must establish objective criteria for selecting the staff that are supposed to be educated in such new developments. After taking the course, these trained persons should educate the other analysts on this new information. This approach may allow the agencies to maintain their budget, while increasing the skill level of the analysts.

Conclusion

This chapter addressed particular solutions for the problems of organized crime analysis units. Solutions were addressed to considering management of information and technology, privacy issues, educational issues, international organizations for information sharing, and managerial issues. Above all, law enforcement agencies must exploit the benefits of technological developments in information analysis, while considering privacy issues. As an international threat, organized crime must be analyzed as a global concern. The exchange of information and experience among law enforcement agencies around the world is a requirement for effective detection and prevention of organized crime.

CHAPTER VI

CONCLUSION AND RECOMMENDATIONS

This study has illustrated the changing nature of organized crime at both national and international levels. In response this change, the use of new analytical tools to modify law enforcement efforts against organized crime is suggested. The reason for this modification is that law enforcement has faced vast amounts of information regarding organized crime activities. International organized crime activities augment the volume of information. For instance, money-laundering activities are increasingly performed among criminal organizations all over the world. This refers to an infinite number of money transactions among national and international banks. Following the financial transactions among the criminal groups with analytical tools, such as link and financial analyses, has been deemed an indispensable tool in understanding the overall picture of organized crime activities. Consequently, this study has presented important and interconnected chapters to address the vital role of crime and intelligence analysis in the fight against the new organized crime problem. These chapters explored the critical points of new organized crime, and suggested the use of crime and intelligence analysis in light of this change.

Although law enforcement agencies take advantage of information technology, they have faced many problems, including costs, expertise, and privacy and security issues. This study offered particular solutions for the problems illustrated in the context, including technological, educational, managerial, and privacy issues.

For technological issues, this study has focused on information management to increase the effectiveness and efficiency of handling this technology. Further, if information technology is managed successfully, departmental budgets may be sufficient to follow the new developments.

In addressing education, this study has concentrated on the professionalism of crime and intelligence analysis to eliminate the difficulties that come from the complexity of using analytical techniques. In terms of professionalism, this study has suggested that universities and colleges reconsider their current curricula in criminal justice programs. New curricula must include specific courses on crime and intelligence analysis. In addition to this, crime and intelligence analysis should be addressed as a unique career in law enforcement with its own system of professional recognition.

For managerial issues, this paper has addressed the critical role of managers in analytical units. The managers must establish consistent and continuous relationships between analysts and field officers. Analysts and officers are often separated in terms of their duties. The responsibility of managers is to provide a proper environment to allow analysts and officers to work together. Managers are also considered responsible for ensuring the proper training of the personnel regarding new advances in analytical techniques. This study has also recommended that managers join International Association of Analysts to share their experiences with other agencies, and to follow new developments.

In addressing privacy issues, this study addressed the standards that protect individual privacy rights, and has presented ways law enforcement agencies should

consider these issues while they handle information technology. Further, the study has emphasized that organizations must determine the level of individual privacy concerns, and take appropriate action to ensure the proper use of information systems in law enforcement efforts. Overall, privacy must be protected without jeopardizing the current investigation.

On the other hand, although crime analysis is considered a method of community policing, it can be adopted for many sophisticated crime. Crime analysis techniques are used for serial murders, robbery, arson, and other crimes. This study showed that crime analysis and intelligence analysis combined would be effective and efficient for organized crime prevention. Specifically, GIS applications can be improved when it is used as a network analysis technique.

Developing information technology is not the main goal. Instead, the goal is to diminish organized criminal activity and enhance preventive methods. Information analysis techniques are integral to the operation of law enforcement agencies. Today, information gathering, accessing, use and dissemination methods are changing commensurate with the intention of agencies to implement more sophisticated technologies.

The argument is that the changes in criminal activities require the same proportional improvement in policing regarding both philosophy and approach. The modifications in policing must be strategic, not simply tactical. This is a significant issue in organized crime policing. More specifically, effective and strategic organized crime policing depends on information gathering and processing systems not used in traditional

policing. Although traditional policing is still important, proactive policing predominantly leads to effective strategies in organized crime prevention.

The Recommendations

This comprehensive study of new organized crime and information analysis leads to a number of recommendations. These recommendations are helpful in considering crime and intelligence analysis, and they also provide effective prevention strategies in the fight against the organized crime.

(1) Concentrate on the relationship between geographic location and organized crime activities. Patterns of organized crime activities regarding to this relationship are likely to provide future trends of criminal organizations. This approach may make decision making process much more effective in establishing prevention policies against organized crime all over the world.

(2) Use practical applications to graphically depict financial transactions by using GIS (Geographical Information System). GIS assists to visualize the money transactions among criminal organizations. Visualization of criminal activities is likely to support strategic analysis in organized crime policing.

(3) Develop new analytical methods for organized crime prevention. GIS is considered a suitable environment to combine crime and intelligence analysis. Increasing number of information requires much more powerful analytical tools.

(4) Develop new and user-friendlier programs for GIS and crime mapping applications to eliminate the difficulties in use. One of the problems in

information analysis is how to relieve the complexity of utilizing software programs. User-friendly programs are likely to eliminate this difficulty. Also, this step must also consider cost-benefit factors in handling new programs.

(5) Clarify the function of GIS. Indeed, GIS does not solve problems itself, but it graphically depicts various information to make more clear and understandable. GIS must be considered a powerful managerial tool in policing.

(6) Advance new tools for information management considering liability, privacy, training, and costs. Up to now, police agencies have become reluctant to utilize these analytical tools due to costs and complexity of. Future technology, therefore, must take these points into considerations.

(7) Expand the use of GIS/GPS integrated system for the purpose of both tactical and strategic intelligence. This system could be used for target tracking and real-time strategic planning. In tracking systems, the less volume of GIS/GPS, the more flexibility the police might have in installing to possible target. Nevertheless, it is not necessary to use the smallest technology in police cars. Again, managers must decide on the proper technology for particular cases. This approach is more likely to reduce the cost in using high technology.

(8) Maintain the role of analysts even if information systems bring more 'intelligent' solutions. Indeed, information systems provide only objective results. Policing organized crime must also take subjective criteria into account. These subjective criteria are determined through human investigation and analysis. Analytical programs, indeed, may on make observation for identifying

relationships. Therefore, some other information must be integrated to each other to be able to recognize the possible conspiracy.

(9) Use expert systems with objective worth and link analysis in tracking the suspicious transactions seen in money laundering investigation. Artificial intelligence techniques must be adapted to this particular situation. Therefore, these analyses may allow law enforcement to track true paths for the relationships within criminals or with other criminal organizations. Also, modified tools may prevent innocent persons from the possible guilty.

(10) Develop an improved GIS project in performing GTO (Geographical Targeting Order), one of the essential methods in money laundering investigation. This study has attempted to apply GIS model for GTO efforts. More importantly, future efforts must concentrate on improving GIS/GTO applications. Essentially, this combination provides the pattern of money transactions with regard to geographic location.

(11) Foster close relationships between police departments and intelligence agencies. This can be accomplished by using uniform analytical tools. In that, the agencies will communicate in the same 'language'. This maintains international cooperation among law enforcement agencies and countries in a suitable format.

(12) Increase the public awareness of organized crime. The public also has an important role in supplying law enforcement with information, especially at local level. Police organizations must obtain the trust to foster this relationship.

In applying the above recommendations, it is felt that combined crime and intelligence analysis (CIA) can be an effective and efficient method in the detection and prevention of organized crime.

References

Abadinsky, H. (1997). Organized crime (5th ed.). Chicago, Illinois: Nelson Hall Inc.

Albanese, J.S. (2000). Causes of organized crime: Do criminals organize around opportunities for crime or do criminal opportunities create new offenders? Journal of Contemporary Criminal Justice, 16 (4), 409-423.

Albanese, J. S. (1996). Organized Crime in America. (3rd ed.) Cincinnati: Anderson Publishing.

Andrews, P. P. Jr. (1990). Collection and analysis plans. Criminal Intelligence Analysis. Paul P. Andrews, Jr. and Marilyn B. Peterson, eds. Loomis, CA: Palmer Enterprises.

Anselin, L., Cohen, J., Cook, D., Gorr, W., & Tita, G. (2000). Spatial analyses of crime. In D. Duffee (Ed.) Measurement and Analysis of Crime and Justice; criminal justice 2000, (Vol. 4, pp. 213-262). [online]. Available: http://www.ncjrs.org/criminal_justice2000/vol_4/04e.pdf (December 2000).

Beare, M.E, & Martens, F.T. (1998). Policing organized crime. Journal of contemporary criminal justice, 14, (4), 398-427.

Boba, R. (2000). Guidelines to implement and evaluate crime analysis and mapping in law enforcement agencies. Community oriented policing services U.S. Department of Justice. [On-line]. Available:

http://www.usdoj.gov/cops/pdf/cp_resources/ppse_pubs/e112k0774.pdf [February 12, 2001].

Joan Z. Bernstein, J. Z. (2000). United States of America federal trade commission. Washington DC, US. [On-line]. Available: http://www.ftc.gov/be/v000013.htm [March 3, 2001].

Bovenberk, F., & Yesilgoz, Y. (2000). Turkiye'nin mafyasi [Turkish mafia]. Istanbul: Iletisim yayinlari.

Brandt, D. (1995). Organized crime threatens the new world order. NameBase Newsline. [On-line]. Available: file://A:\org_future.htm [January 8, 2001].

The Bureau for International Narcotics and Law Enforcement Affairs, U.S. Department of State. (1998). International narcotics control strategy report, 1997: Money laundering and financial crimes. [On-line]. Available: http://www.state.gov/www/global/narcotics_law/1998_narc_report/ml_intro.html [February 13, 2001].

Canter, P. (1995). State of the statistical art: Point-pattern analysis. In C.R. Block, M. Dabdoub, & S. Fregly (Eds.), Crime analysis through computer mapping, (pp. 151-160). Washington, DC: Police research forum, Criminal justice press.

Carter, D.L. (2001). International organized crime. Unpublished paper. [On-line]. Available: http://www.cj.msu.edu/~outreach/security/orgcrime.html [February 9, 2001].

Chantler, N., & Wigan, B. (1993). Intelligence and: The development of accredited courses. Unpublished paper, Australia: Queensland institute of technology, Brisbane.

CMRC. (2001). [On-line]. Available: http://www.ojp.usdoj.gov/cmrc/tools/welcome.html [February 13, 2001].

Dempsey, C. (2001). Crime mapping: GIS goes mainstream. Geographical information systems. [On-line]. Available: wysiwyg://139/http://www.gis.about…/library/weekly/aa101100.htm [February 9, 2001]

Denning, D.E, & Baugh, W.E. (1997). Encryption and evolving technologies as tools of organized crime and terrorism. [On-line]. Available: http://www.cs.georgetown.edu/~denning/crypto/cases.html [April 2, 2000].

Dintino, J. J. & Martens, F.T. (1981). An enduring enigma: The concept of intelligence analysis. Police Chief, 48, (12), 58-64.

Dintino, J. J. & Martens, F.T. (1983). Police intelligence systems in crime control. Springfield, IL: Charles C. Thomas.

Dunworth, T. (2000). Criminal justice and the IT revolution. In J. Horney, (Ed.), Policies, Processes, and Decisions of the Criminal Justice System; Criminal Justice ***2000*** (pp. 371-426). [On-line]. Available: http://www.ncjrs.org/criminal_justice2000/vol_3/03h.pdf [September 15, 2000].

Europol. (1998). Crime analysis in the view of europol. [On-line]. Available: http://www.bka.de/aktuell/analtikertagung/kriminalpolizeiliche_auswetung.html [September 15, 2000].

Evans, L. A. (1997). Investigating and prosecuting the proceeds of crime: A common law experience. In E. U. Savona, (Ed.), Responding to money laundering:

International perspectives (pp. 189-214). Amsterdam, the Netherlands: Harwood Academic Publishers.

Fahlman, R. (2000). Intelligence led policing and the key role of criminal intelligence analysis: Preparing for the 21st century. [On-line]. Available: http://www.interpol.int/Public/cia/fahlman.asp [September 28, 2000].

Feldman, M. (2001). The Reagan information interchange. [On-line]. Available: http://www.reagan.com/HotTopics.main/HotMike/document-12.18.1997.5.html [March 3, 2001].

Louis, F.J. (1999). The fight against transnational organized crime. In D.L. Bender, B. Leone, B. Stalcup, S. Barbour, & J.D. Torr, (Eds.), Organized crime (pp. 161-167). San Diego, CA: Greenhaven Press, Inc.

Froomkin, A.M. (1996). The metaphor is the key: Cryptography, the clipper, and the constitution. [On-line]. Available: http://www.law.miami.edu/~froomkin/articles/clipper.htm [March 7, 2001].

Frost, C.C. (1985). Choosing Good Intelligence Analysts: What's Measurable? Law Enforcement Intelligence Analysis Digest, 1 Summer/Fall, 1-11.

Gill, P. (1998a). Police intelligence processes: A study of criminal intelligence units in Canada. Policing and Society, 8, pp. 339-365.

Gill, P. (1998b). Making sense of police intelligence? The use of a cybernetic model in analyzing information and power in police intelligence processes. Policing and Society, 8, pp 289-314.

Gist, N.E. (1998). Regional information sharing systems program. Bureau of justice assistance fact sheet. [On-line]. Available: http://www.ncjrs.org/txtfiles/fs000037.txt [January 14, 2001].

Global justice information network annual report. (2000). Institute for intergovermental research. [On-line]. Available: http://www.iir.com/global/report.htm [March 3, 2001].

Godfrey, E. Drexel and Don R. Harris. (1971). Basic elements of intelligence. Washington, D.C.: U.S. Government Printing Office.

Godson, R., & Olson W. J. (1995). International organized crime. Society, 32, (2), 18-29.

Goldberg, I., Wagner, D., & Brewer, E. (2001). Privacy-enhancing technologies for the Internet. University of California, Berkeley. [On-line]. Available: http://www.cs.berkeley.edu/~daw/papers/privacy-compcon97-www/privacy-html.html [February 4, 2001].

Goodwin, B. (September 2000). New Met system will target crime hot spots. Computer weekly.

Gottlieb, S., Arenberg, S., Singh, R. (1994). Crime Analysis from first report to final arrest. California, US: Alpha Publishing.

Haley, K.N., Todd, J.C., & Stallo, M. (March 1998). Crime analysis and the struggle for legitimacy. Unpublished and presented at ACJS Annual Meeting. [On-line]. Available: http://www.iaca.net/resources/FAQs/FAQ%20…..20Struggle%20for%20Legitimacy.htm

Harries, K. (2000). Mapping crime: Principle and practice. [On-line]. Available: http://www.ncjrs.org/html/nij/mapping/pdf.html [September 14, 2000].

Harris, D.R. (1976). Basic elements of intelligence (Rev. ed.). Washington, D.C. U.S.: Government Printing Office.

Godfrey, E. D., & Harris, R. D. (1971). Basic elements of intelligence. Washington DC: Law Enforcement Assistance Administration.

Heaton, R. (2000). The prospects for intelligence-led Policing: Some historical and quantative considerations. Policing and society, 9, pp. 337-355.

Heuer, R.J. (1999). Psychology of intelligence analysis. Center for the study of intelligence. [On-line]. Available: http://www.cia.gov/csi/books/19104/ [February 13, 2001].

Hicks, D.C. (1998). Thinking about organized crime prevention. Journal of contemporary criminal justice, 14, 4, 325-350.

Ianni, F.A.J., & Ianni, E. R. (1990). Network analysis. In P. P. Andrews, & M.B. Peterson, (Eds.), Criminal Intelligence Analysis. Loomis, CA: Palmer Enterprises.

IALEIA. (2001). [On-line]. Available: http://www.ialeia.org/about.html [February 13, 2001].

IC: The Intelligence Community in the 21st Century, Staff Study. (1996). [On-line]. Available: http://sun00781.dn.net/irp/congress/1996 rpt/ic21/report.html. [October 25, 2000].

Information and privacy office. (1999). Privacy impact assessment guidelines. [On-line]. Available: http://www.gov.on.ca/MBS/english/fip/pia/ [February 13, 2001].

Information Industry Association. (2001). Fair information practices guidelines: Policy statement. [On-line]. Available: http://www.privacyexchange.org/buscodes/iap/multi/infoia.html [January 5, 2001].

Levi, M. (1998). Perspectives on 'organized crime': An overview. The Howard Journal, 37 (4), 335-345.

Lodha, S.K., & Verma, A. (1999). Animations of crime maps using virtual reality modeling language. Western criminology review, 1 (2). [On-line]. Available: http://wcr.sonoma.edu/v1n2/lodha.html [February 9, 2001].

Lupsha, P. A. (1980). Steps toward a strategic analysis of organized crime. Police Chief, 47 (4).

McDowell, D., Wardlaw, G., & Schmidt, J. (1991). A model for the development of strategic crime assessments. Canberra, Australia: Attorney-General's Department of Australia.

Manning, G.A. (1999). Financial investigation and forensic accounting. London, UK: CRC Press.

MapInfo. (2001). [On-line]. Available: http://www.mapinfo.com/ [March3, 2001].

Martens T. F, & Dintino J.J. (December 1981). An enduring enigma: The concept of intelligence analysis. The Police Chief, pp. 58-64.

Martens, F. T. (1986). An enforcement paradox: The intelligence dilemma in narcotic enforcement. Journal of Justice Issues, 1, (2).

Martens, F. T. (1987). The intelligence function. In H. Edelhertz, (Ed.), Major Issues in Organized Crime Control, (pp. 26-39). Washington, D.C.: U.S. Department of Justice, National Institute of Justice.

Martens, F.T. (1990). The intelligence function. In P.P. Andrews, & M.B. Peterson, (Eds.), Criminal intelligence analysis (pp. 1-20). Loomis, US: Palmer enterprises.

Maguire, M. (2000). Policing by risks and targets: some dimensions and implications of intelligence-led-crime control. Policing and Society, 9, 315-336.

Mennecke, B.E. (1997). Understanding the role of geographic information technologies in business: Applications and research directions. Journal of geographical information and decision analysis, 1, (1), 44-68.

Milhaupt, C.J., & West, M.D. (2000). The dark side of private ordering: An institutional and empirical analysis of organized crime. The university of Chicago law review, 67, (1), 41-97.

Norris, C., & Dunninghan, C. (2000). Subterranean blues: Conflict as a unintended consequence of the police use of informers. Policing and Society, 9, 385-412.

Olligschlaeger, A.M. (May 1997). Spatial analysis of crime using GIS-based data: Weighted spatial adaptive filtering and chaotic cellular forecasting with applications to street level drug markets. A Dissertation submitted to the H.John Heinz III School of Public policy and management, Carnegie Mellon University. [On-line]. Available: http;//cs.cmu.edu/~olli/dissertation.html [September 15, 2000].

Peterson, M. B (1990). Telephone Record Analysis. In P. Andrews, & M.B. Peterson, (Eds.), Criminal Intelligence Analysis (pp.85-115). Loomis, CA: Palmer Enterprises.

Peterson, M. B. (1994). Intelligence and Analysis Within the organized crime Function. In R. J. Kelly, K.L. Chin & R. Schatzberg, Handbook of Organized crime, (eds.), (pp. 359-387). California: Greenwood Press.

Peterson, M.B. (1997). Practical analytical techniques: A necessary addition to police education. Journal of Criminal Justice Education, 8, (1), 19-35.

Peterson, M.B. (1998). Applications in criminal analysis: A sourcebook. London, UK: Praeger.

Police intelligence. (October 1999). USAMPS white paper 00-05. [On-line]. Available: http://wood.army.mil/usamps/dot/Doctrine/White%20Papers/PI.htm [June 27, 2000].

Politi, A. (October 1997). European security: The new transnational risks. Institute for Security Studies Western European Union, Chaillot Paper 29. Paris. [On-line]. Available: http://www.weu.int/institute/chaillot/chai29e.htm. [April 24, 2000].

Prunckun, H. W. (1990). Special Access Required: A Practitioner's Guide to Law Enforcement Intelligence Literature. Metuchen, NJ: Scarecrow Press.

Prunckun, H.W. (1996). The intelligence analyst as social scientist: A comparison of research methods. Police studies, 19, (3), 67-80.

Royal Canadian Mounted Police (1998). RCMP criminal Intelligence Program Guide: Roles and functions. Ottawa, Ontario, Canada: Royal Canadian Mounted Police.

Reuland, M. (1997). Information management and crime analysis. Washington, D.C.: Police Executive Research Forum. [On-line], http://www.iaca.net [September 25, 2000].

Rich, T.F. (1995). The use of computerized mapping in crime control and prevention programs. NIJ research in action. [On-line]. Available: http://communitypolicing.org/eleclib/txfiles/riamap.txt [February 28, 2001].

Richards, J. R. (1999). Transnational criminal organizations, cybercrime, and money laundering Baco Raton, Florida: CRC Press LLC.

Rucker, B.R. (1995). The criminal intelligence: enforcing today, managing tomorrow. The Police Chief, 62, 34.

Rossmo, D.K. (2000). Geographic Profiling. CRC Press.

Sherman, L.W. (1995). Hot spots of crime and criminal careers of places. In J. E Eck & D. Weisburd (Eds.), Crime and Place, (pp. 35-52). Monsey, United States: Criminal Justice Press/Willow Tree Press.

Schneider, Stephen. (June 1994). The criminal intelligence function: Toward a Comprehensive and Normative Model. Law Enforcement Intelligence Analyst Digest, 9, (2), 1-26.

Shelley, L.L. (1995). Transnational organized crime: An imminent threat to the nation-state? Journal of International Affairs, 48, (2), 463-489.

Sheptycki, J. (2000). Editorial reflections on surveillance and intelligence-led policing. Policing and Society, 9, pp. 311-314.

Sommers, M. (1986). Law enforcement intelligence, a new look. International Journal of Intelligence and Counterintelligence, 1, (3), 25-40.

Sorensen, S.L. (1997). Smart mapping for law enforcement settings: Integrating GIS and GPS for dynamic, near-real time applications and analysis. In D. Weisburd & T. McEwen (Eds.), Crime Mapping and Crime Prevention, (pp. 349-378). Monsey, United states: Criminal justice press.

Sparrow K. M. (1991). The application of network analysis to criminal intelligence: An assessment of the prospects. Social Networks, 13, pp. 251-274.

Sparrow, M. K. (1991). Network vulnerabilities and strategic intelligence in law enforcement. International Journal of Intelligence and Counterintelligence, 5, (3). 24-57.

Stewart, J.G. (December 2000). Intelligence analysis of transnational crime: Assessing Canadian preparedness. [On-line]. Available: http://www.lib.unb.ca/Texts/JCS/S96/articles/stewart.html [December 17, 2000]

Stockley, D. (1988). National drugs intelligence unit. Police Journal, 61, (4), 13-21.

Stallo, M. 1997. Crime analysis: The administrative function. In M. Stallo, & K. Haley, (Eds.), Crime and Punishment in the Lone Star State (pp. 63-76). New York: McGraw-Hill, Inc.

Swanson, C., Leonard T., & Taylor, R.W. (2000). Police administration structures, process, and behavior. (fifth. ed.). Prentice Hall, New Jersey.

Taylor, R.W. (1987). Terrorism and intelligence. Defense analysis, 3, (2), 165-175.

Criminal intelligence service Canada. (2000). Technology and crime. [On-line]. Available: http://www.cisc.gc.ca/Cisc2000/technology2000.html [January 10, 2001].

United Nations. (1999). Global studies on organized crime. Vienna. [On-line]. Available: http://www.uncjin.org/Special/gsoc_e.pdf [January 25, 2000].

United States Department of Justice. (2000). Privacy impact for justice information systems working paper. [On-line]. Available: http://www.ojp.usdoj.gov/integratedjustice/piajis.htm [February 28, 2001]

Williams, Phil. (1995). Transnational criminal organizations: Strategic alliances. The Washington Quarterly. 18, (1), winter: 57.

Wolf, John B. (1978). The Police Intelligence System. New York, US: John Jay (CUNY) Press.

Wong, C. (1997). Web client programming with perl: Automating tasks on the web. O'Reilly open books project. [On-line]. Available: http://www.oreilly.com/openbook/webclient/toc.html [February 7, 2001].

Zoufal, D. R. (2000). Legal issues in law enforcement information sharing. Police chief, 67, (12), 8-10.